
VE RI TS
SIGILLVM ACADEMIAE HARVARDIANAE IN NOV ANG
CHRISTO ET ECCLESIAE



VORLESUNGEN

ÜBER

ALGEBRA

VON

DR. EUGEN NETTO,

O. Ö. PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT ZU GIESSEN.

IN ZWEI BÄNDEN.

ZWEITER BAND.

MIT EINGEDRUCKTEN HOLZSCHNITTEN.

LEIPZIG,

DRUCK UND VERLAG VON B. G. TEUBNER.

1900.

Vorwort.

Der vorliegende zweite und letzte Band meiner „Vorlesungen über Algebra“ umfasst zwei getrennte, von einander weit verschiedene Stoffe, die Theorie der Elimination und diejenige der höheren Gleichungen einer Unbekannten. Ein Abschluss konnte, wie dies ja für ein wissenschaftliches Werk naturgemäss ist, in keinem der beiden Abschnitte erreicht werden; aber bei der Behandlung der Elimination liess sich nach der Richtung eine gewisse Vollständigkeit erreichen, als die hauptsächlichsten Resultate der bisherigen auf diesem Gebiete angestellten Untersuchungen besprochen und verwerthet wurden; es sind wohl kaum wichtigere Forschungen über die Elimination unerwähnt geblieben. Eine kurze Theorie der ganzen Functionen mehrerer Veränderlichen musste vorausgehen, in welcher die Grundeigenschaften, die Irreductibilitätsfragen, die Wurzeln ganzer Functionen besprochen wurden. Hierher hätte wohl auch eine eingehende Darstellung der Modulsysteme gehört; doch glaubte ich von dieser absehen zu müssen, da die schwierigen Fragen, welche dabei auftauchen, noch nicht hinlänglich ihre Beantwortung gefunden haben. Bei der Theorie der Elimination wurden die Hauptmethoden behandelt. In der Bezeichnung folgte ich den englischen Forschern, indem ich zwischen „Resultante“ und „Eliminante“ sorgfältig unterschied.

Lässt es sich auch nicht durchaus rechtfertigen, diesen Abschnitt an die Stelle gesetzt zu haben, an welcher er steht, so blieb doch kaum eine Wahl, da seine Resultate sich auf das Vorhergehende stützen und beim Nachfolgenden benutzt werden.

Bei der Besprechung der höheren Gleichungen einer Unbekannten musste, aus Gründen des Raumes, sowohl auf eine Berücksichtigung a l l e r werthvollen Forschungen in den behandelten Gebieten, als auch auf eine Darlegung a l l e r ihrem Wesen nach hergehöriger Gebiete verzichtet werden. Es war dies dem Verfasser um so weniger angenehm, als dadurch die Behandlung von Fragen bei Seite geschoben werden musste, die in neuester Zeit wesentlich gefördert wurde und eine abgeschlossene Darstellung erlaubt hätte. Vielleicht wird es ihm möglich

sein, in anderer Weise die gebliebenen Lücken auszufüllen. Dass bei dieser Lage der Abschluss des ganzen Werkes etwas Willkürliches aufweist, ist nur zu erklärlich; aber ein genaues Eingehen zeigt, dass dieser Mangel auch beim Weiterschreiten sich nicht hätte beseitigen lassen, da aller Orten am Ausbau der Theorien gearbeitet wird.

Das Heranziehen der Gruppen- und der Substitutionentheorie, welches im ersten Bande und auch im ersten Abschnitte des zweiten Bandes vermieden werden konnte, war hier eine Nothwendigkeit. Ich habe versucht, Alles was von dieser Theorie gebracht werden musste, in unmittelbare Beziehung zu den algebraischen Gleichungen zu setzen, selbst wenn dabei manches interessante und für andere Zweige der Wissenschaft durchaus wichtige Theorem unberücksichtigt bleiben musste. Mit einigem Widerstreben habe ich in diesem Abschnitte eine vielfach neue Nomenclatur benutzt; es galt den Versuch, etwas schwerfällige Bezeichnungen durch bequemere zu ersetzen; und leider ist die Mannigfaltigkeit in den Benennungen zur Zeit noch eine so grosse, es haben sich einheitliche Bräuche so wenig ausgebildet, dass der Versuch wenigstens nicht als etwas ganz Besonderes bezeichnet werden kann.

Auch in diesem Bande habe ich die Literaturangaben möglichst vollständig zu liefern gesucht.

Giessen.

Eugen Netto.

Inhaltsverzeichniss.

Vierter Abschnitt.

Gleichungen mit mehreren Unbekannten (Vorlesung 30—48).

I. Functionen mehrerer Variablen (Vorlesung 30—32).

II. Elimination (Vorlesung 33—47).

III. Der Hilbert'sche Irreductibilitätssatz (Vorlesung 48).

Fünfter Abschnitt.

Allgemeine Theorie der algebraischen Gleichung unter Verwendung der Substitutionengruppen (Vorlesung 49—68).

I. Cyklische und Abel'sche Gleichungen (Vorlesung 49—50).

II. Gruppen und Functionengattungen (Vorlesung 51—59).

III. Algebraische Zahlen; Radicalzahlen (Vorlesung 60—65).

IV. Anwendungen der Theorie (Vorlesung 66—68).

Dreissigste Vorlesung.

Ganze Functionen mehrerer Variablen.

§ 327. Die Behandlung von Gleichungen höherer Grade hat uns von selbst auf Functionen mehrerer Variablen, nämlich auf solche der verschiedenen Wurzeln dieser Gleichungen geführt. Wir kommen jetzt zunächst zu einer systematischen Untersuchung der Eigenschaften von ganzen Functionen beliebig vieler Veränderlichen und dann zur Behandlung von Gleichungssystemen beliebig vieler Unbekannten.

Ein Ausdruck von der Form

$$(1)\qquad f(z_1, z_2, z_3, \cdots) = \sum_{\alpha,\beta,\gamma,\cdots} c_{\alpha,\beta,\gamma,\cdots} z_1^\alpha z_2^\beta z_3^\gamma \cdots$$

$$(\alpha = 0, 1, \cdots r_1;\ \beta = 0, 1, \cdots r_2;\ \gamma = 0, 1, \cdots r_3;\ \cdots),$$

in welchem die $r_1, r_2, r_3, \cdots$ ganze positive Zahlen, und die $c_{\alpha,\beta,\gamma,\cdots}$ Grössen eines gegebenen Rationalitätsbereiches bezeichnen, soll eine ganze rationale Function der Veränderlichen $z_1, z_2, z_3, \cdots$ innerhalb des festgesetzten Rationalitätsbereiches heissen. Die einzelnen Terme $z_1^\alpha z_2^\beta z_3^\gamma \cdots$ nennen wir Potenzproducte der Variablen.

Je nach der Anzahl der Veränderlichen unterscheiden wir ganze Functionen von einer, zwei, drei, $\cdots$ Variabeln. Eine ganze Function von m Variablen kann in die Form einer ganzen Function einer einzigen dieser Variablen gebracht werden, deren Coefficienten ganze Functionen der $(m-1)$ anderen Variablen sind,

$$(1^a)\quad f(z_1, z_2, z_3, \cdots) = \sum_\alpha \varphi_\alpha(z_2, z_3, \cdots) z_1^\alpha, \qquad (\alpha = 0, 1, \cdots r_1);$$

ebenso in die Form einer ganzen Function von zwei dieser Variablen, deren Coefficienten ganze Functionen der übrigen sind,

$$(1^b)\qquad f(z_1, z_2, z_3, \cdots) = \sum_{\alpha,\beta} \psi_{\alpha,\beta}(z_3, \cdots) z_1^\alpha z_2^\beta$$

und in gleicher Weise weiter.

§ 328. Die höchste Potenz, zu welcher eine Variable in f aufsteigt, giebt den Grad der Function nach dieser Variablen an. So ist in (1) der Grad von f nach z_1 gleich r_1, nach z_2 gleich r_2, u. s. f.

Unter der Dimension der ganzen Function f verstehen wir den höchsten Werth, welchen die Summe $(\alpha + \beta + \gamma + \cdots)$ der Grade in den einzelnen Potenzproducten annimmt. Die Dimension kann die Summe der Grade nicht übertreffen.

Haben die Summen $(\alpha + \beta + \gamma + \cdots)$ in allen einzelnen Potenzproducten denselben Wert n, so heisst die Function homogen von der Dimension n. Für eine homogene Function (1) der Dimension n gilt bekanntlich der Euler'sche Satz

$$z_1 \frac{\partial f}{\partial z_1} + z_2 \frac{\partial f}{\partial z_2} + z_3 \frac{\partial f}{\partial z_3} + \cdots = nf.$$

§ 329. Kommen alle überhaupt bei einer ganzen Function n^{ter} Dimension von m Variablen möglichen Glieder in f vor, so nennen wir f eine vollständige ganze Function. Eine solche Function hat für $m = 1$ gerade $(n + 1)$ Glieder. Bei zwei Variablen z_1, z_2 kommen als mit $z_2^{n-\alpha}$ multiplicirt $(\alpha + 1)$ Glieder vor; da nun α von 0 bis n gehen kann, so beträgt die gesamte Anzahl der Glieder $\frac{(n+1)(n+2)}{1 \cdot 2}$. In derselben Art kann man schrittweise fortgehen und findet durch Induction, wenn $N(n, m)$ die Anzahl der möglichen Potenzproducte n^{ter} Dimension von m Variablen bedeutet, die Formel

$$(2) \qquad \begin{aligned} N(n, m) &= \frac{(n+1)(n+2)\cdots(n+m)}{1 \cdot 2 \cdots m} = \binom{n+m}{m} \\ &= \frac{(m+1)(m+2)\cdots(m+n)}{1 \cdot 2 \cdots n} = \binom{m+n}{n}. \end{aligned}$$

Es ist $N(n, 0) = N(0, m) = 1$. Für negative Werte eines oder beider Argumente wollen wir die Verabredung treffen, dem N den Wert 0 beizulegen, weil dadurch die Formeln sich einfacher gestalten.

§ 330. Jetzt untersuchen wir, wieviele der Potenzproducte einer vollständigen Function n^{ter} Dimension der m Variablen $z_1, z_2, \cdots z_m$ durch $z_1^{a_1}$ teilbar sind $(a_1 \leqq n)$. Man erkennt sofort, dass, wenn man aus allen diesen Gliedern $z_1^{a_1}$ herauszieht, die zurückbleibenden Potenzproducte alle Glieder einer vollständigen ganzen Function derselben Variablen von der Dimension $(n - a_1)$ bilden müssen. Die Anzahl der gesuchten Glieder beträgt demnach $N(n - a_1, m)$.

Ebenso findet man für die Anzahl der Potenzproducte, welche als Factor $z_1^{a_1} z_2^{a_2}$ enthalten $(a_1 + a_2 \leqq n)$, den Wert $N(n - a_1 - a_2, m)$, u. s. f. Die Bedingungen $a_1 \leqq n$, $a_1 + a_2 \leqq n_1, \cdots$ können gemäss der letzten Festsetzung des vorigen Paragraphen unterdrückt werden.

Aus diesen Resultaten kann man ohne Schwierigkeit entnehmen, wieviel Glieder von $f(z_1, z_2, \cdots z_m)$ der n^{ten} Dimension durch keins der Monome

$$z_1^{a_1}, z_2^{a_2}, \cdots z_m^{a_m} \qquad (a_i \geqq 1)$$

theilbar sind, oder, wieviele Glieder in z_1 höchstens bis zum Grade $(a_1 - 1)$, in z_2 höchstens bis zum Grade $(a_2 - 1), \cdots$ aufsteigen. Ist ein a gleich 1, dann darf also die entsprechende Variable überhaupt nicht vorkommen. — Subtrahirt man von der Anzahl $N(n, m)$ aller in f auftretenden Potenzproducte die Summe aus der Anzahl derer, die $z_1^{a_1}$ enthalten, derer die $z_2^{a_2}$ enthalten, u. s. w. und bezeichnet man diese Summe

$$(3) \quad N(n - a_1, m) + N(n - a_2, m) + \cdots + N(n - a_m, m) = S_1,$$

so bleibt in der Zahl

$$(4) \qquad N(n, m) - S_1$$

der restirenden Glieder keins der auszuschliessenden zurück. Jedoch sind dabei die durch $z_1^{a_1} z_2^{a_2}$ theilbaren Potenzproducte zweimal fortgenommen worden, einmal unter den durch $z_1^{a_1}$ theilbaren und einmal unter den durch $z_2^{a_2}$ theilbaren. Alle diese Glieder, deren Zahl $N(n - a_1 - a_2, m)$ beträgt, sind daher einmal zu addiren. Das Gleiche gilt von den Combinationen $z_1^{a_1} z_3^{a_3}, \cdots z_{m-1}^{a_{m-1}} z_m^{a_m}$. Die obige Differenz ist also um

$$(5) \qquad \sum_{\alpha,\beta} N(n - a_\alpha - a_\beta, m) = S_2$$

zu erhöhen, wobei die Summe sich auf alle Combinationen α, β ohne Wiederholung der Zahlen $1, 2, \cdots m$ bezieht. Jetzt sind alle, nur zwei Variable enthaltenden Potenzproducte richtig gestellt. Hingegen sind z. B. die durch $z_1^{a_1} z_2^{a_2} z_3^{a_3}$ theilbaren in $N(n, m)$ einmal enthalten gewesen, durch S_1 dreimal in Fortfall gekommen, durch S_2 dann wieder dreimal zugefügt, so dass sie also schliesslich noch einmal weggenommen werden müssen. Das sind also $N(n - a_1 - a_2 - a_3, m)$ Glieder. So sind im Ganzen noch

$$(6) \qquad \sum_{\alpha,\beta,\gamma} N(n - a_\alpha - a_\beta - a_\gamma, m) = S_3$$

Glieder zu subtrahiren, u. s. w.

Man erkennt, dass die benutzten Schlüsse genau dieselben sind, wie die, welche wir § 302, Bd. I verwendet haben, um die Form der Kreistheilungsgleichung zu bestimmen. Die hier gesuchte Anzahl ergiebt sich auf gleichem Wege als

$$(7) \qquad N(n, m) - S_1 + S_2 - S_3 + \cdots + (-1)^m S_m.$$

Nimmt man sämmtliche a gleich 1, so entsteht hieraus

$$N(n,m)-1=mN(n-1,m)-\binom{m}{2}N(n-2,m)+\binom{m}{3}N(n-3,m)-\cdots.$$

§ 331. Wir bezeichnen, wie dies in der Differenzenrechnung gebräuchlich ist, für ein positives oder verschwindendes α

$$N(n, m) - N(n-\alpha, m) = \Delta_\alpha N(n, m). \tag{8}$$

Dann ist

$$\begin{aligned} N(n, m) - [N(n-\alpha, m) + N(n-\beta, m)] + N(n-\alpha-\beta, m) \\ = \Delta_\alpha N(n, m) - \Delta_\alpha N(n-\beta, m) = \Delta_{\alpha,\beta} N(n, m) \\ = \Delta_\beta N(n, m) - \Delta_\beta N(n-\alpha, m) = \Delta_{\beta,\alpha} N(n, m). \end{aligned}$$

Statt $\Delta_{\alpha,\beta}$ oder $\Delta_{\beta,\alpha}$ werden wir auch $\Delta^{(2)}_{\alpha,\beta}$ oder $\Delta^{(2)}_{\beta,\alpha}$ schreiben, um anzudeuten, falls dies nöthig ist, dass zwei untere Indices vorkommen; und das soll in gleicher Weise allgemein gemacht werden.

Diese Einführungen ermöglichen es, den Ausdruck (7) kurz

$$\Delta^{(m)}_{a_1, a_2, \cdots a_m} N(n, m) \tag{7^a}$$

zu schreiben. Die unteren Indices a können dabei willkürlich permutirt werden.

§ 332. Für die eingeführten Symbole besteht eine bemerkenswerthe Beziehung, die jetzt abgeleitet werden soll. Die Addition der bekannten Formeln

$$\begin{aligned} &N(n, m) &&- N(n-1, m) &&= N(n, m-1), \\ &N(n-1, m) &&- N(n-2, m) &&= N(n-1, m-1), \\ &\cdots \\ &N(n-a_1+1, m) &&- N(n-a_1, m) &&= N(n-a_1+1, m-1) \end{aligned}$$

liefert die Summe

$$\Delta_{a_1} N(n, m) = \sum_{\eta=0}^{a_1-1} N(n-\eta, m-1).$$

Hierbei braucht a_1 nicht der Beschränkung $a_1 \leqq n$ unterworfen zu werden.

Durch die Anwendung der Operation Δ_{a_2} entsteht hieraus für beliebige a_1, a_2

$$\begin{aligned} \Delta^{(2)}_{a_1, a_2} N(n, m) &= \sum_{\eta=0}^{a_1-1} \Delta_{a_2} N(n-\eta, m-1) \\ &= \sum_{\eta, \varkappa} N(n-\eta-\varkappa, m-2) \quad \binom{\eta=0,1,\cdots a_1-1}{\varkappa=0,1,\cdots a_2-1}. \end{aligned}$$

Ebenso erhält man aus dieser Formel durch die Anwendung der Operation Δ_{a_3} weiter

$$\Delta^{(3)}_{a_1, a_2, a_3} N(n, m) = \sum N(n - \eta - \varkappa - \lambda, \; m - 3)$$
$$(\eta = 0, 1, \cdots a_1 - 1; \; \varkappa = 0, 1, \cdots a_2 - 1; \; \lambda = 0, 1, \cdots a_3 - 1),$$

und in derselben Weise kann man fortfahren, so dass allgemein entsteht

$$(9) \quad \Delta^{(\varrho)}_{a_1, a_2, \cdots a_\varrho} N(n, m) = \sum N(n - \eta_1 - \eta_2 - \cdots - \eta_\varrho, m - \varrho)$$
$$(\eta_1 = 0, 1, \cdots a_1 - 1; \cdots \eta_\varrho = 0, 1, \cdots a_\varrho - 1).$$

In diese Formel tragen wir jetzt $\varrho = m$ ein, wodurch das zweite Argument von N zu Null gemacht wird. So oft dann das erste Argument nicht negativ ist, so oft wird der entsprechende Summand den Wert 1 annehmen, während er sonst gleich Null wird. Ist also

$$(a_1 - 1) + (a_2 - 1) + \cdots + (a_m - 1) = \sum a_\lambda - m \leq n,$$

so ist jeder Summand gleich 1, und da $a_1 \cdot a_2 \cdots a_m$ Summanden bestehen,

$$(9^a) \quad \Delta^{(m)}_{a_1, a_2, \cdots a_m} N(n, m) = a_1 \cdot a_2 \cdots a_m \qquad \left(\sum a_\lambda - m \leqq n\right).$$

Ist $\sum a_\lambda - m = n + 1$, dann liefert der eine auf

$$\eta_1 = a_1 - 1, \quad \eta_2 = a_2 - 1, \quad \cdots \quad \eta_m = a_m - 1$$

bezügliche Summand den Wert 0, die anderen stets den Wert 1 und daher ist

$$(9^b) \quad \Delta^{(m)}_{a_1, a_2, \cdots a_m} N(n, m) = a_1 \cdot a_2 \cdots a_m - 1 \quad \left(\sum a_\lambda - m = n + 1\right).$$

Bei $\sum a_\lambda - m = n + 2$ liefern die $(m + 1)$ Summanden

$$\eta_1 = a_1 - 1, \quad \eta_2 = a_2 - 1, \quad \cdots \quad \eta_m = a_m - 1;$$
$$\eta_1 = a_1 - 1, \cdots \eta_{\lambda-1} = a_{\lambda-1} - 1, \; \eta_\lambda = a_\lambda - 2, \; \eta_{\lambda+1} = a_{\lambda+1} - 1, \cdots$$
$$(\lambda = 1, \; 2, \; \cdots \; m)$$

den Wert Null, so dass entsteht

$$(9^c) \quad \Delta^{(m)}_{a_1, a_2, \cdots a_m} N(n, m) = a_1 \cdot a_2 \cdots a_m - (m + 1) \quad \left(\sum a_\lambda - m = n + 2\right).$$

Ebenso erhält man

$$(9^d) \quad \Delta^{(m)}_{a_1, a_2, \cdots a_m} N(n, m) = a_1 \cdot a_2 \cdots a_m - (m^2 + 1) \quad \left(\sum a_\lambda - m = n + 3\right)$$

und in ähnlicher Weise weiter. Zu beachten ist aber bei diesen Rechnungen, dass in (9^c) z. B. keins der a kleiner als 2, in (9^d) keins kleiner als 3 vorausgesetzt ist.

§ 333. Es seien wie oben

$$z_1^{a_1},\ z_2^{a_2},\ \cdots\ z_m^{a_m}$$

gegebene Monome, und ζ_ν bezeichne die Anzahl der Potenzproducte aus f, welche durch ν und auch nur durch ν dieser Monome teilbar sind. Nun umfasst S_1 die Zahl aller Potenzproducte, die durch eins der Monome teilbar sind, und ausserdem alle, die durch zwei unter ihnen theilbar sind, doppelt; alle, die durch drei unter ihnen theilbar sind, dreifach u. s. w. Es ist daher

$$S_1 = \zeta_1 + 2\zeta_2 + 3\zeta_3 + 4\zeta_4 + \cdots + m\zeta_m,$$

und ebenso folgt

$$(10)\qquad \begin{aligned} S_2 &= \zeta_2 + 3\zeta_3 + 6\zeta_4 + \cdots + \binom{m}{2}\zeta_m, \\ S_3 &= \qquad\ \zeta_3 + 4\zeta_4 + \cdots + \binom{m}{3}\zeta_m, \\ &\cdots\cdots\cdots\cdots\cdots \\ S_m &= \qquad\qquad\qquad\quad \binom{m}{m}\zeta_m. \end{aligned}$$

Hieraus ergiebt sich

$$(10^a)\qquad \begin{aligned} S_1 - S_2 + S_3 - S_4 + S_5 - \cdots &= \zeta_1 + \zeta_2 + \zeta_3 + \zeta_4 + \cdots + \zeta_m, \\ S_2 - S_3 + S_4 - S_5 + \cdots &= \zeta_2 + 2\zeta_3 + 3\zeta_4 + \cdots + \binom{m-1}{1}\zeta_m, \\ S_3 - S_4 + S_5 - \cdots &= \zeta_3 + 3\zeta_4 + \cdots + \binom{m-1}{2}\zeta_m, \\ S_4 - S_5 + \cdots &= \zeta_4 + \cdots + \binom{m-1}{3}\zeta_m, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

so dass also sämmtliche links stehende Differenzen positive Werthe haben. Weiter liefert das erste System auch umgekehrt

$$(10^b)\qquad \begin{aligned} \zeta_1 &= S_1 - 2S_2 + 3S_3 - 4S_4 + \cdots + (-1)^{m-1} m S_m, \\ \zeta_2 &= \qquad S_2 - 3S_3 + 6S_4 - \cdots + (-1)^m \binom{m}{2} S_m, \\ \zeta_3 &= \qquad\qquad S_3 - 4S_4 + \cdots + (-1)^{m-1}\binom{m}{3} S_m, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

Die Formeln (7) und (7ᵃ) zeigten, dass

$$N(n, m) - \Delta^{(m)}_{a_1, a_2, \cdots a_m} N(n, m) = S_1 - S_2 + S_3 - \cdots + (-1)^{m-1} S_m$$

ist. Aus (10ᵃ) folgt, dass $(S_2 - S_3 + \cdots)$ positiv sein muss; demnach wird

(11) $$S_1 > N(n, m) - \Delta^{(m)}_{a_1, \cdots a_m} N(n, m).$$

Als besonderer Fall ergiebt sich hieraus vermittels (9ᵃ)

(11ᵃ) $$\sum_{\lambda=1}^{m} N(n - a_\lambda, m) > N(n, m) - a_1 \cdot a_2 \cdots a_m \qquad \left(\sum a \leq n + m\right).$$

Diese letzte Bedingung ist für $n = a_1 \cdot a_2 \cdots a_m$ erfüllt, sobald die a wenigstens zum Theil grösser als 1 sind.

§ 334. Wir betrachten jetzt wieder eine vollständige Function der m Variablen $z_1, z_2, \cdots z_m$ von der Dimension n; sie hat $N(n,m)$ Terme. Aus ihnen wollen wir alle diejenigen hinwegstreichen, die durch eins der Monome

$$z_1^{a_1}, \; z_2^{a_2}, \; z_3^{a_3}, \; \cdots \; z_m^{a_m}$$

theilbar sind, und aus den zurückbleibenden noch alle diejenigen, welche von der $(n - a_{m+1})^{\text{ten}}$ oder von einer geringeren Dimension sind. Die Bestimmung der Anzahl der restirenden Potenzproducte geschieht genau nach der Methode des § 330. Zunächst nämlich erkennt man, dass in f gerade $N(n - a_{m+1}, m)$ Glieder von geringerer als der $(n - a_{m+1} + 1)^{\text{ten}}$ Dimension sind. Ferner ist die Anzahl der Glieder von geringerer als der $(n - a_{m+1} + 1)^{\text{ten}}$ Dimension, welche durch $z_1^{a_1}$ theilbar sind, gleich $N(n - a_1 - a_{m+1}, m)$, u. s. f. Es sind also die Voraussetzungen, auf welche die Schlüsse von § 330 beruhten, hier gewahrt. Bezeichnen wir daher

$$\Sigma_1 = \sum_{\lambda=1}^{m+1} N(n - a_\lambda, m),$$

$$\Sigma_2 = \sum_{\lambda, \mu=1}^{m+1} N(n - a_\lambda - a_\mu, m),$$

$$\cdots\cdots\cdots\cdots$$

so folgt für die gesuchte Anzahl der Wert

(12) $$N(n, m) - \Sigma_1 + \Sigma_2 - \Sigma_3 + \cdots + (-1)^{m+1} \Sigma_{m+1}.$$

Die Verschiedenheit zwischen (7) und (12) liegt zu Tage.

Gesetzt es wäre

$$(a_1 - 1) + (a_2 - 1) + \cdots + (a_m - 1) \leq n - a_{m+1},$$

dann bleiben in $f(z_1, \ldots)$ überhaupt keine Terme zurück. Denn das Glied höchster Dimension, welches durch keins der festgelegten Monome theilbar ist, lautet $z_1^{a_1-1} z_2^{a_2-1} \cdots z_m^{a_m-1}$ und fällt also bereits unter diejenigen, welche ihrer Dimensionszahl wegen zu streichen sind.

Das zeigt: Der Werth von (12) ist gleich Null, wenn

$$a_1 + a_2 + \cdots + a_{m+1} \leq n + m.$$

Falls dagegen

$$a_1 + a_2 + \cdots + a_{m+1} = n + m + 1$$

ist, beträgt der Werth von (12) Eins, da dann offenbar $z_1^{a_1-1} z_2^{a_2-2} \cdots z_m^{a_m-1}$ von der Dimension $n + 1 - a_{m+1}$ das einzige zurückbleibende Glied ist.

Ist weiter

$$a_1 + a_2 + \cdots + a_{m+1} = n + m + 2,$$

dann ist der Werth von (12) gleich $(m + 1)$, denn jetzt bleiben ausser $z_1^{a_1-1} z_2^{a_2-1} \cdots z_m^{a_m-1}$ noch die Glieder zurück, die aus ihm durch Division mit z_1, oder $z_2, \ldots$ oder z_m entstehen. Natürlich ist hierbei die Voraussetzung zu machen, dass jedes der a mindestens gleich 1 ist.

Die weiteren hierher gehörenden Schlüsse übergehen wir.

§ 335. Wir bezeichnen nun mit ξ_ν die Anzahl derjenigen Glieder unseres Polynoms f, welche genau ν und nur ν der im vorigen Paragraphen aufgestellten $(m + 1)$ Bedingungen erfüllen. So ist z. B. ξ_1 die Anzahl der Potenzproducte, welche nur durch eins der Monome theilbar und zugleich von höherer als der $(n - a_{m+1})^{\text{ten}}$ Dimension sind, vermehrt um die Anzahl derjenigen, die von niederer als der $(n - a_{m+1})^{\text{ten}}$ Dimension, aber durch keins der Monome theilbar sind.

Entsprechend den Formeln (10) aus § 333 gilt hier

$$(13)\quad \begin{aligned}
\Sigma_1 &= \xi_1 + 2\xi_2 + 3\xi_3 + 4\xi_4 + \cdots + (m+1)\,\xi_{m+1},\\
\Sigma_2 &= \xi_2 + 3\xi_3 + 6\xi_4 + \cdots + \binom{m+1}{2}\xi_{m+1},\\
\Sigma_3 &= \xi_3 + 4\xi_4 + \cdots + \binom{m+1}{3}\xi_{m+1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\Sigma_{m+1} &= \binom{m+1}{m+1}\xi_{m+1}.
\end{aligned}$$

Daraus folgt dann weiter

$$(13^a)\quad \begin{aligned}
\Sigma_1 - \Sigma_2 + \Sigma_3 - \Sigma_4 + \cdots &= \xi_1 + \xi_2 + \xi_3 + \cdots + \xi_{m+1},\\
\Sigma_2 - \Sigma_3 + \Sigma_4 - \cdots &= \xi_2 + 2\xi_3 + \cdots + m\xi_{m+1},\\
\Sigma_3 - \Sigma_4 + \cdots &= \xi_3 + \cdots + \binom{m}{2}\xi_{m+1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

Da nun nach dem vorigen Paragraphen (12) für $\sum_1^{m+1} a_\lambda \leq n + m$ den

Werth 0 hat, so folgt, weil die Ausdrücke (13ᵃ) nicht negativ sind, wie aus den rechten Seiten ersichtlich ist, in diesem Falle

$$
\begin{aligned}
\Sigma_1 - N(n,m) &= \Sigma_2 - \Sigma_3 + \cdots \geqq 0, \\
(\Sigma_1 - N(n,m)) - \Sigma_2 &= -\Sigma_3 + \Sigma_4 - \cdots < 0, \qquad (14) \\
(\Sigma_1 - N(n,m)) - \Sigma_2 + \Sigma_3 &= \Sigma_4 - \Sigma_5 + \cdots \geqq 0, \\
\cdots & \cdots
\end{aligned}
$$

Das untere Zeichen kann dabei nur auftreten, wenn beim Abschlusse auf der linken Seite mit $\pm \Sigma_\alpha$ alle $\xi_{\alpha+1}, \xi_{\alpha+2}, \ldots$ verschwinden. Aus der Bedeutung der ξ folgt dann, dass jeder der Ausdrücke in (14) mit Ausnahme des letzten unter ihnen das obere Vorzeichen erhalten muss; der letzte dagegen das untere.

§ 336. Aus (13) folgt, ähnlich wie früher,

$$\Sigma_1 - 2\Sigma_2 + 3\Sigma_3 - 4\Sigma_4 + \cdots + (-1)^m \Sigma_{m+1} = \xi_1.$$

Wir wollen den Werth von ξ_1 unter der Voraussetzung bestimmen, dass

$$a_1 + a_2 + \cdots + a_m + a_{m+1} \leqq n + m$$

sei. Dazu bringen wir alle Glieder von f, so weit dies nöthig ist, unter Einführung einer neuen Variablen u, durch Multiplication mit einer passenden Potenz von u auf die Dimension n. Dann wird jedes Glied, welches vorher von der $(n - a_{m+1})^{\text{ten}}$ oder von einer niedrigeren Dimension war, jetzt durch $u^{a_{m+1}}$ theilbar geworden sein. Folglich umfasst in der umgeänderten Function die Zahl ξ_1 alle diejenigen Glieder, welche durch eins und auch nur durch eins der Monome

$$z_1^{a_1}, z_2^{a_2}, \cdots z_m^{a_m}, u^{a_{m+1}}$$

theilbar sind. Um zunächst zu finden, wieviele durch $z_1^{a_1}$ allein theilbar sind, aber durch keins der anderen Monome, bilden wir die Producte aus je einer Potenz von z_2, von $z_3, \ldots$ und von u aus den Reihen

$$1, z_2, \cdots z_2^{a_2-1};\ 1, z_3, \cdots z_3^{a_3-1};\ \cdots;\ 1, u, \cdots u^{a_{m+1}-1}.$$

Jedes so erhaltene Product hat eine Dimension kleiner oder gleich

$$a_2 + a_3 + \cdots + a_{m+1} - m \leqq n - a_1;$$

multiplicirt man es also mit einer Potenz von z_1, die es auf die n^{te} Dimension bringt, so hat diese einen Exponenten $\geqq a_1$, d. h. wir haben eins der gewünschten Glieder erhalten. Es giebt also $a_2 \cdot a_3 \cdots a_{m+1}$ solche, den verschiedenen Combinationen entsprechend. Ebenso finden wir für alle durch $z_2^{a_2}$ und durch keins der anderen Monome theilbaren Potenzproducte die Zahl $a_1 \cdot a_3 \cdots a_{m+1}$, u. s. w. Das ergiebt also

$$(15)\quad \Sigma_1 - 2\Sigma_2 + 3\Sigma_3 - \cdots + (-1)^m \Sigma_{m+1} = \sum_{\lambda=1}^{m+1} \frac{a_1 \cdot a_2 \cdots a_{m+1}}{a_\lambda}$$
$$\left(\sum_1^{m+1} a_\lambda \leqq n + m\right).$$

Auf weitere Formeln wollen wir nicht eingehen; (15) ist lediglich zu späterem Gebrauche abgeleitet worden. Es mag nur noch erwähnt werden, dass sich die an (7) und (12) anknüpfenden Untersuchungen verallgemeinern lassen und so zu interessanten Ergebnissen führen.

Einunddreissigste Vorlesung.

Fundamentaleigenschaften ganzer Functionen von mehreren unabhängigen Variablen. Reductibilität. Zerlegung.

§ 337. Die bisherigen Untersuchungen bezogen sich auf den formalen Aufbau der ganzen Functionen mehrerer Veränderlichen; jetzt kommen wir zu ihren Fundamentaleigenschaften.

Verschwindet die ganze Function

$$(1)\qquad f(z_1, z_2, \cdots z_m) = \sum_{\alpha, \beta, \gamma, \cdots} c_{\alpha, \beta, \gamma, \cdots} z_1^\alpha z_2^\beta z_3^\gamma \cdots$$
$$(\alpha = 0, 1, \cdots r_1;\quad \beta = 0, 1, \cdots r_2;\quad \gamma = 0, 1, \cdots r_3; \cdots)$$

für jedes beliebige Werthsystem $(z_1, z_2, \cdots z_m) = (\zeta_1, \zeta_2, \cdots \zeta_m)$, dann sind alle Coefficienten c gleich Null, und umgekehrt.

Der zweite Teil des Satzes ist selbstverständlich. Den ersten beweisen wir zunächst durch strenge Induction. Wir setzen

$$f(z_1, z_2, \cdots z_m) = \sum_\alpha \varphi_\alpha(z_2, z_3, \cdots z_m) z_1^\alpha$$

und nehmen an, der zu beweisende Satz gelte für Functionen von $(m-1)$ Variablen $z_2, z_3, \cdots z_m$. Legen wir nun den $z_2, \cdots z_m$ ein ganz beliebiges Werthsystem $\zeta_2, \cdots \zeta_m$ bei und dem z_1 dann mehr als r_1 Werthe $\zeta_1', \zeta_1'', \cdots$, so müssen alle Coefficienten $\varphi_\alpha(\zeta_2, \zeta_3, \cdots \zeta_m)$ verschwinden, da $f(z_1, \zeta_2, \cdots \zeta_m) = 0$ mehr als r_1 Wurzeln $\zeta_1', \zeta_1'', \cdots$ besitzt. Das Gleiche gilt für alle Werthsysteme $\zeta_2, \zeta_3, \cdots \zeta_m$; d. h. die $\varphi_\alpha(z_2, z_3, \cdots z_m)$ verschwinden für jedes willkürliche System der $z_2, z_3, \cdots z_m$. Gemäss der angenommenen Gültigkeit des Satzes sind dann alle Coefficienten

der φ, d. h. auch die von f gleich Null. Für $m = 1$ ist der Satz richtig; demnach gilt er allgemein.

Aus dem Gange des Beweises folgt die Erweiterung: Ist (1) für jede der $(r_1 + 1)(r_2 + 1) \cdots (r_m + 1)$ Combinationen von

$$\begin{array}{l} z_1 = \zeta_1', \ \zeta_1'', \ \cdots \ \zeta_1^{(r_1+1)} \\ z_2 = \zeta_2', \ \zeta_2'', \ \cdots \ \zeta_2^{(r_2+1)} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ z_m = \zeta_m', \ \zeta_m'', \ \cdots \ \zeta_m^{(r_m+1)} \end{array}$$

gleich Null, so verschwinden in f alle Coefficienten $c_{\alpha,\beta,\gamma,\cdots}$.

§ 338. Wir wollen für den ersten dieser Sätze einen weiteren Beweis geben, der sich auf eine Bemerkung von L. Kronecker*) stützt. Wir setzen, indem wir unter q eine noch zu bestimmende ganze positive Zahl verstehen,

$$(2) \qquad z_1 = t, \quad z_2 = t^q, \quad z_3 = t^{q^2}, \quad z_4 = t^{q^3}, \ \ldots ;$$

dadurch geht das Potenzproduct

$$z_1^\alpha z_2^\beta z_3^\gamma \cdots \quad \text{in} \quad t^{\alpha + \beta q + \gamma q^2 \cdots}$$

über. Es handelt sich jetzt zunächst darum, Fürsorge dafür zu treffen, dass zu verschiedenen Systemen $\alpha, \beta, \gamma, \cdots$ auch verschiedene Zahlenwerthe des Exponenten von t, nämlich $\alpha + \beta q + \gamma q^2 + \cdots$ gehören. Ist r die grösste der Zahlen $r_1, r_2, \cdots r_m$, welche die Grade von f in $z_1, z_2, \cdots z_m$ angeben, dann wählen wir $q > r + 1$. Daraus folgt der Reihe nach

$$\begin{array}{l} q^2 > qr + q > qr + r = r(q+1), \\ q^3 > q^2 r + q^2 > q^2 r + qr + r = r(q^2 + q + 1), \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ q^m > q^{m-1} r + q^{m-1} > r(q^{m-1} + q^{m-2} + \cdots + q + 1). \end{array}$$

Gesetzt nun, man hätte die Gleichheit zweier Ausdrücke

$$\alpha + \beta q + \gamma q^2 + \cdots + \varepsilon q^m = \alpha_1 + \beta_1 q + \gamma_1 q^2 + \cdots + \varepsilon_1 q^m,$$

und es wäre etwa $\varepsilon \geqq \varepsilon_1$, dann ergäbe sich daraus

$$(\varepsilon - \varepsilon_1) q^m = (\alpha_1 - \alpha) + (\beta_1 - \beta) q + (\gamma_1 - \gamma) q^2 + \cdots.$$

Nun sind $(\alpha_1 - \alpha)$, $(\beta_1 - \beta)$, $\cdots$ nicht grösser als r, und folglich

$$(\varepsilon - \varepsilon_1) q^m < r(1 + q + q^2 + \cdots + q^{m-1}) < q^m,$$

---

*) Grundzüge einer arithmetischen Theorie der algebraischen Grössen § 4. J. f. M. 92 (1882). p. 1.

d. h. $\varepsilon = \varepsilon_1$. Aehnlich folgert man dann weiter und erkennt, dass aus der angenommenen Gleichheit der beiden Ausdrücke in q die Gleichheit aller Exponenten folgt.

Nach diesen Vorbereitungen gehen wir auf den zu beweisenden Satz zurück. Die Substitution (2) verwandelt (1) in eine ganze Function $\varphi(t)$ von t, welche nicht identisch verschwindet, wenn dies nicht bei (1) der Fall ist. Denn nach unseren Vorbereitungen können nicht mehrere Glieder von (1) denselben Exponenten in t erlangen. Die umgewandelte Function kann nur für eine endliche Anzahl von Werthen verschwinden, wenn sie nicht identisch Null ist. Nach der Voraussetzung des Satzes ist aber (1) gleich Null für $z_{\alpha+1} = \tau^{q^\alpha}$, wo τ beliebig genommen werden kann; also ist die Gleichung $\varphi(t) = 0$ in t für jedes $t = \tau$ erfüllt, d. h. sämmtliche Coefficienten von $\varphi(t)$ und also auch von $f(t)$ sind gleich Null.

Der hier benutzte Uebergang von Functionen mit mehreren zu solchen mit einer Variablen wird sich uns auch noch in der Folge als nützlich erweisen.

§ 339. Wenn ein Product aus ganzen, rationalen Functionen mehrerer Veränderlichen für jedes beliebige System $z_1, z_2, \cdots z_m$ der m Variablen verschwindet, dann verschwindet einer seiner Factoren identisch.

Wir führen die Kronecker'sche Substitution (2) durch, sorgen bei ihr aber auch dafür, dass in dem Producte selbst keine gleichen Exponenten von t auftreten, was ja für hinlänglich grosse q leicht zu erreichen ist. Verschwindet nun das ursprüngliche Product für jede Wahl der Variablen, dann verschwindet auch das umgewandelte, in dem nur eine Veränderliche t auftritt, für jeden Wert dieses t. Das ist allein dann möglich, wenn einer der Factoren in t identisch verschwindet, da andernfalls jeder derselben nur für eine endliche Anzahl von Werthen t zu Null würde. Ist aber ein Factor in t identisch Null, dann ist es auch die Function, aus welcher er hervorgegangen war.

§ 340. Wir müssen noch eine Substitution besprechen, durch welche (1) in eine neue Form übergeht, in der sie nun von gewissen Zufälligkeiten frei wird, die aus den Werthen der Constanten entspringen können.

Wir setzen die linearen Gleichungen an

$$(3)\qquad \begin{aligned} z_1 &= u_{11} y_1 + u_{12} y_2 + \cdots + u_{1m} y_m, \\ z_2 &= u_{21} y_1 + u_{22} y_2 + \cdots + u_{2m} y_m, \\ &\cdots\cdots\cdots\cdots\cdots \\ z_m &= u_{m1} y_1 + u_{m2} y_2 + \cdots + u_{mm} y_m, \end{aligned}$$

wobei vorläufig über die Wahl der Coefficienten u nur die Bestimmung getroffen werden soll, dass die Determinante $\Delta = | u_{\lambda\mu} |$ von Null verschieden sei, damit auch umgekehrt

$$(4) \qquad \begin{aligned} y_1 &= v_{11} z_1 + v_{21} z_2 + \cdots + v_{m1} z_m, \\ y_2 &= v_{12} z_1 + v_{22} z_2 + \cdots + v_{m2} z_m, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ y_m &= v_{1m} z_1 + v_{2m} z_2 + \cdots + v_{mm} z_m \end{aligned}$$

gesetzt werden kann. Durch diese Substitution möge

$$f(z_1, z_2, \cdots z_m) = \varphi(y_1, y_2, \cdots y_m)$$

werden, d. h. es ist zu setzen

$$\varphi = \sum c_{\alpha, \beta, \gamma, \ldots} (u_{11} y_1 + \cdots + u_{1m} y_m)^\alpha (u_{21} y_1 + \cdots + u_{2m} y_m)^\beta \cdots .$$

Hier bilden die Glieder, welche in $y_1, y_2, \cdots$ den höchsten, nämlich den n^{ten} Grad besitzen, die Summen

$$y_1^n \sum c_{\alpha, \beta, \ldots} u_{11}^\alpha u_{21}^\beta \cdots \quad \text{bez.} \quad y_2^n \sum c_{\alpha, \beta, \ldots} u_{12}^\alpha u_{22}^\beta \cdots, \text{ u. s. f.},$$

wobei die Summation über alle Glieder erstreckt werden muss, für welche die Summe der Exponenten $\alpha, \beta, \cdots$ den Werth n besitzt. Diese c können nicht sämmtlich verschwinden, denn sonst wäre f nicht von der n^{ten} Dimension. Man kann daher (§ 337) beliebig viele Werthsysteme $u_{1\alpha}, u_{2\alpha}, \cdots u_{m\alpha}$ bestimmen, für welche das Product

$$| u_{\lambda\mu} | \cdot \sum c_{\alpha, \beta, \ldots} u_{11}^\alpha u_{21}^\beta \cdots \sum c_{\alpha', \beta', \ldots} u_{12}^{\alpha'} u_{22}^{\beta'} \cdots$$

nicht verschwindet. Dadurch haben wir eine umkehrbare lineare Substitution (2) erhalten, durch deren Vermittelung aus f eine Function $\varphi(y_1, y_2, \cdots y_m)$ hervorgeht, welche sicher alle Glieder $y_1^n, y_2^n, \cdots y_m^n$ mit nicht verschwindenden Coefficienten multiplicirt enthält. Der Grad in jeder der Variablen ist gleich der Dimension der Function geworden.

Liegen mehrere Functionen $f(z_1, \cdots z_m)$, $g(z_1, \cdots z_m)$, $\cdots$ vor, und wendet man auf ihr Product $f \cdot g \cdots$ unsere Transformation an, so entsteht ein Product $\varphi(y_1, \cdots y_m) \cdot \psi(y_1, \cdots y_m) \cdots$, in welchem jedes y_α die Dimension des Productes hat. Dies ist natürlich nur dann möglich, wenn die gleiche Eigenschaft schon bei jeder einzelnen der Functionen vorhanden ist. Man kann also eine umkehrbare Substitution finden, durch welche beliebig viele Functionen gleichzeitig in der angegebenen Weise zubereitet werden.

§ 341. Ist die Function (1) in der Form eines Productes

$$f = g(z_1, z_2, \cdots) \cdot h(z_1, z_2, \cdots)$$

darstellbar, wobei g, h gleichfalls ganze Functionen aber von geringeren Dimensionen bedeuten, deren Coefficienten genau wie die von f einem vorgegebenen Rationalitätsbereiche angehören, dann heisst (1) reductibel oder zerlegbar in die Factoren g und h. Ist eine Function f nicht reductibel, dann heisst sie irreductibel oder unzerlegbar.

Es ist hier darauf aufmerksam zu machen, dass im Gegensatze zu Functionen mit einer Veränderlichen jetzt auch bei beliebiger Erweiterung des Rationalitätsbereiches eine Zerfällung in lineare Factoren nicht nothwendig eintreten muss, sondern dass eine solche nur nach Erfüllung von gewissen Bedingungen zwischen den Coefficienten eintreten kann. So ist z. B.

$$a_{11}z_1^2 + 2a_{12}z_1z_2 + a_{22}z_2^2 + 2a_{13}z_1 + 2a_{23}z_2 + a_{33}$$

nur dann in lineare Factoren zerfällbar, wenn

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{vmatrix} = 0$$

ist. Auf diese Frage wollen wir aber hier nicht eingehen*).

Wir geben zunächst eine Methode an, wie eine Function f darauf hin geprüft werden kann, ob sie reductibel oder irreductibel ist, und wie man im ersten Falle ihre Factoren finden kann.

Führen wir die Kronecker'sche Substitution (2) in f durch, dann erhalten wir dadurch eine Function $F(t)$ einer Variablen t, welche sicher reductibel wird, falls f es ist, während das Umgekehrte nicht richtig zu sein braucht. $F(t)$ kann nun nach früher angegebenen Methoden auf alle Arten in zwei Factoren zerlegt werden. Ist f reductibel, dann muss einer Zerlegung von f eine solche von F derart entsprechen, dass die Factoren von f durch (2) in die von F übergeführt werden. Bei Irreductibilität von F steht also die Irreductibilität von f gleichfalls fest. Hat dagegen $F(t)$ den Theiler

$$\chi(t) = \sum \varrho_\lambda t^{\sigma_\lambda},$$

dann fragt es sich, ob dieses $\chi(t)$ durch (2) überhaupt aus einer ganzen Function $g(z_1, z_2, \cdots z_m)$ hervorgehen kann. Dazu müsste es möglich sein, jeden Exponenten σ_λ in die Form

$$\sigma_\lambda = \alpha_\lambda + \beta_\lambda q + \gamma_\lambda q^2 + \cdots + \varepsilon_\lambda q^{m-1} \qquad (\alpha_\lambda \leqq r_1, \quad \beta_\lambda \leqq r_2, \cdots)$$

zu setzen. Wir wissen (§ 338), dass dies höchstens auf eine Weise

*) Ueber die Zerfällung von Ternärformen vgl. Aronhold: J. f. M. 55 (1858), p. 97. Brioschi: Ann. d. M. (2) 7 (1875—76), p. 189. Thaer: Math. Ann. 14 (1879), p. 545. Brill: Math. Ann. 50 (1898), p. 157.

möglich ist, so dass $\chi(t)$ höchstens aus einer einzigen Function g entstanden sein kann. Diese Function wird dann

$$g = \sum \varrho_\lambda z_1^{\alpha_\lambda} z_2^{\beta_\lambda} z_3^{\gamma_\lambda} \cdots$$

sein. Man hat demnach nur noch die einzelnen so erhaltenen Functionen g darauf hin zu prüfen, ob sie Theiler von f sind; denn ausser ihnen kann es keine Theiler von f geben. Dadurch wird die Entscheidung über die Irreductibilität geliefert, und zugleich wird eine Zerlegung bestimmt, falls eine solche überhaupt vorhanden ist. Die Prüfung geht theoretisch am einfachsten derart vor sich, dass man zuerst alle g bestimmt und dann je zwei, die passende Dimensionen besitzen, zur Probe mit einander multiplicirt. Die Prüfung durch directe Division ist an dieser Stelle aus theoretischen Gründen noch nicht angängig.

§ 342. Dass die Zerlegung einer Function f in irreductible Factoren wesentlich nur auf eine einzige Art möglich ist, können wir auf dem betretenen Wege nicht beweisen. Zu diesem Fundamentalsatze gelangen wir durch eingehendere Betrachtungen. Wir werden ihn als Corollar aus dem folgenden Theoreme ableiten: Ist das Product $f_1(z_1, z_2, \cdots) f_2(z_1, z_2, \cdots)$ durch eine irreductible Function $g(z_1, z_2, \cdots)$ theilbar, dann ist einer der Factoren f_1 oder f_2 durch g theilbar.

Für $m = 1$ steht die Richtigkeit dieses Satzes fest (§ 68, Bd. I); seine allgemeine Gültigkeit kann also durch Induction bewiesen werden. Wir wollen deshalb annehmen, er sei schon für $(m-1)$ Veränderliche als richtig erkannt. Daraus wollen wir einige Folgerungen ziehen, die uns dann zum Beweise desselben Satzes für m Veränderliche führen werden.

Zunächst ziehen wir aus der Annahme den Schluss, dass Functionen von $(m-1)$ Veränderlichen nur auf wesentlich eine Art in irreductible Factoren zerlegt werden können.

Denn wäre

$$f(z_1, \cdots z_{m-1}) = g_1 \cdot g_2 \cdots g_\mu = h_1 \cdot h_2 \cdots h_\nu,$$

wobei die g und die h ganze irreductible Functionen von $z_1, z_2, \cdots z_{m-1}$ bedeuten, so ist $h_1 \cdot (h_2 \cdots h_\nu)$ durch g_1 theilbar, und also der Annahme nach auch entweder h_1 oder $(h_2 \cdots h_\nu)$. Sollte es $(h_2 \cdots h_\nu)$ sein, so wiederholen wir den gleichen Schluss bei $h_2 \cdot (h_3 \cdots h_\nu)$ u. s. f. Es ist also ein h durch g_1 theilbar, und da dies h selbst irreductibel ist, so muss es mit g_1 bis auf einen constanten Factor übereinstimmen. Es wird demnach etwa $h_1 = c_1 \cdot g_1$, und durch Division erhält man

$$g_2 \cdot g_3 \cdots g_\mu = c_1 \cdot h_2 \cdot h_3 \cdots h_\nu.$$

Fährt man in derselben Weise fort, dann überzeugt man sich von der Richtigkeit des Satzes.

§ 343. Jetzt beweisen wir die folgenden Sätze:

(I) Ist $f(z_1, z_2, \cdots z_m)$ durch $\varphi(z_2, z_3, \cdots z_m)$ theilbar, so ist jeder Coefficient der nach Potenzen von z_1 geordneten Function f

$$f = \psi_0(z_2, z_3, \cdots z_m) + \psi_1(z_2, z_3, \cdots z_m) \cdot z_1 + \psi_2(z_2, z_3, \cdots z_m) \cdot z_1^2 + \cdots$$

durch $\varphi(z_2, \cdots z_m)$ theilbar. Denn der Voraussetzung gemäss besteht eine ganze Function $g(z_1, \cdots z_m)$, für welche die Gleichung

$$f = \varphi(z_2, \cdots z_m) \cdot g(z_1, z_2, \cdots z_m)$$

gilt. Entwickelt man g nach Potenzen von z_1 und führt die Multiplication durch, so erkennt man die Richtigkeit des Satzes, da eine Function f von z_1 nur auf eine Art nach Potenzen von z_1 entwickelt werden kann.

(II) Ist das Product $f_1(z_1, \cdots z_m) \cdot f_2(z_1, \cdots z_m)$ durch die irreductible Function $\varphi(z_2, \cdots z_m)$ theilbar, dann sind mindestens bei einem der Factoren f_1 oder f_2 alle Coefficienten der nach z_1 geordneten Function durch φ theilbar.

Denn setzen wir

$$f_1 = \psi_0(z_2, \cdots z_m) + \psi_1(z_2, \cdots z_m) \cdot z_1 + \psi_2(z_2, \cdots z_m) z_1^2 + \cdots,$$
$$f_2 = \chi_0(z_2, \cdots z_m) + \chi_1(z_2, \cdots z_m) \cdot z_1 + \chi_2(z_2, \cdots z_m) z_1^2 + \cdots,$$

so wollen wir annehmen, dass $\psi_0, \psi_1, \cdots \psi_{\alpha-1}$ und $\chi_0, \chi_1, \cdots \chi_{\beta-1}$ durch φ theilbar seien, dagegen ψ_α und χ_β nicht. Nun müsste mit $f_1 \cdot f_2$ auch

$$(f_1 - \psi_0 - \cdots - \psi_{\alpha-1} z_1^{\alpha-1})(f_2 - \chi_0 - \cdots - \chi_{\beta-1} z_1^{\beta-1})$$
$$= \psi_\alpha \chi_\beta \cdot z_1^{\alpha+\beta} + (\psi_\alpha \chi_{\beta+1} + \chi_\beta \psi_{\alpha+1}) z_1^{\alpha+\beta+1} + \cdots$$

durch φ theilbar sein, und somit nach (I) auch $\psi_\alpha \cdot \chi_\beta$. Nach dem für $(m - 1)$ Variable als richtig vorausgesetzten Theorem geht das nicht, wenn ψ_α und χ_β durch φ nicht theilbar sind. Die Existenz eines durch φ nicht theilbaren Coefficientenproducts $\psi_\alpha \cdot \chi_\beta$ ist also nicht möglich, d. h. alle Coefficienten einer der Functionen f_1, f_2 sind durch φ theilbar.

(III) Ist $f_1(z_1, \cdots z_m) \cdot f_2(z_1, \cdots z_m)$ durch die Function $\varphi(z_2, \cdots z_m)$ theilbar, so ist jeder irreductible Factor von φ entweder ein Theiler aller Coefficienten von f_1 oder von f_2. Das bleibt richtig, auch wenn ein solcher irreductibler Factor in höherer Multiplicität bei φ auftritt, derart, dass er in derselben Multiplicität in den beiden Coefficientensystemen zusammen vorhanden ist.

Ist z. B. $\omega(z_2, \cdots z_m)$ ein irreductibler Factor von φ, so gilt von ihm der Satz (II); hebt man ihn dann aus φ und der passend gewählten der beiden Functionen f weg, so kann man mit den zurückbleibenden Factoren von φ ebenso verfahren.

(IV) Ist ein Product $f_1(z_1, \cdots z_m) \cdot \varphi(z_2, \cdots z_m)$ durch $f_2(z_1, \cdots z_m)$ theilbar, wo die nach z_1 geordnete Function f_2 keinen gemeinsamen Theiler in ihren Coefficienten enthält, dann ist f_1 durch f_2 theilbar. Denn aus

$$f_1(z_1, z_2, \cdots z_m) \cdot \varphi(z_2, \cdots z_m) = f_2(z_1, \cdots z_m) \cdot g(z_1, \cdots z_m)$$

folgt, dass $f_2 \cdot g$ durch φ theilbar ist. Nach (III) kann man nun jeden irreductiblen Factor von φ, so oft er vorkommt, aus $f_2 \cdot g$, also nach unserer Voraussetzung aus g wegheben. Ist so φ vollständig herausgehoben, dann zeigt die zurückbleibende Gleichung, dass f_1 durch f_2 theilbar ist.

(V) Ist $f(z_1, z_2, \cdots z_m)$ in zwei Factoren zerlegbar, die in z_1 ganz und in $z_2, \cdots z_m$ rational aber gebrochen sind, dann giebt es auch eine Zerlegung von f, in welcher beide Factoren ganze Functionen von $z_1, z_2, \cdots z_m$ sind. (Vgl. § 48, Bd. I.) Wir bringen in der vorliegenden Zerlegung die beiden gebrochenen Factoren auf die Form

$$\frac{f_1(z_1, z_2, \cdots z_m)}{\varphi_1(z_2, \cdots z_m)} \quad \text{und} \quad \frac{f_2(z_1, z_2, \cdots z_m)}{\varphi_2(z_2, \cdots z_m)},$$

in welcher die f und die φ ganze Functionen der angegebenen Argumente bedeuten, derart, dass f_1 durch keinen Factor von φ_1, und f_2 durch keinen Factor von φ_2 theilbar ist. Nach (II) muss dann, weil $f_1 \cdot f_2$ durch $\varphi_1 \cdot \varphi_2$ getheilt werden kann, f_1 die gesammte Function φ_2 und f_2 ebenso die gesammte Function φ_1 als Factor enthalten. Nach (I) kann man also aus den Coefficienten von f_1 und von f_2 herausheben φ_2 und bez. φ_1. Dadurch gelangt man zu einer Zerlegung von f, welche lediglich ganze Factoren in $z_1, z_2, \cdots z_m$ aufweist.

§ 344. Nach diesem letzten Resultate (V) brauchen wir bei der Zerlegung von f nur darauf zu achten, dass die Factoren ganze Functionen einer der Variablen, z. B. von z_1 sind. Ist der Rationalitätsbereich der natürliche, d. h. umfasst er allein die rationalen ganzen Zahlen, so reicht es aus, alle ganzen ganzzahligen Factoren der gegebenen ganzen ganzzahligen Function zu suchen.

Daraufhin lässt sich eine zweite Methode zur Aufsuchung der irreductiblen Factoren einer ganzen ganzzahligen Function (1) gründen, welche eine Erweiterung der Kronecker'schen Methode für $k = 1$ darstellt (vgl. § 50, Bd. I).

Es möge f bis zur Dimension $n = 2\nu$ oder $n = (2\nu + 1)$ aufsteigen. Nach § 340 denken wir uns die Function gleich so zubereitet, dass n mit dem Grade der Function in z_1 übereinstimmt, dass also der Coefficient von z_1^n in f eine Constante $\neq 0$ wird. Dadurch beseitigen wir die Möglichkeit, dass f einen von z_1 unabhängigen Factor enthält. Ist f überhaupt zerlegbar, dann hat es einen Factor, dessen Grad in z_1 grösser als Null, aber nicht grösser als ν ist. Wir wollen einen solchen Factor als vorhanden annehmen und ihn mit $g(z_1, \cdots z_m)$ bezeichnen. Dann ist für jeden ganzzahligen Werth z_1' der Werth $f(z_1', z_2, \cdots z_m)$ ein Multiplum von $g(z_1', z_2, \cdots z_m)$. Liegt also bereits eine Methode vor, Functionen von $(m - 1)$ Variablen $z_2, \cdots z_m$ in irreductible Factoren zu zerlegen, dann können wir alle Theiler von $f(z_1', z_2, \cdots z_m)$ aufstellen und wissen, dass sich $g(z_1', z_2, \cdots z_m)$ unter ihnen befinden muss. Nun möge für

z_1' die Function $f(z_1', z_2, \cdots)$ die Theiler $d_1'(z_1', z_2, \cdots)$, $d_1''(z_1', z_2, \cdots), \cdots$
z_1'' „ „ $f(z_1'', z_2, \cdots)$ „ „ $d_2'(z_1'', z_2, \cdots)$, $d_2''(z_1'', z_2, \cdots), \cdots$
. . . .
$z_1^{(\nu+1)}$ „ $f(z_1^{(\nu+1)}, z_2, \cdots)$ „ „ $d_{\nu+1}'(z_1^{(\nu+1)}, z_2, \cdots)$, $d_{\nu+1}''(z_1^{(\nu+1)}, z_2, \cdots) \cdots$

besitzen. Die Function $g(z_1, z_2, \cdots)$ muss dann für $z_1 = z_1', z_1'', \cdots$ eine Werthcombination

$$d_1^{(\alpha)}(z_1', z_2, \cdots), \quad d_2^{(\beta)}(z_1'', z_2, \cdots), \cdots$$

aufweisen. Legt man alle Combinationen $\alpha, \beta, \cdots$, die überhaupt möglich sind, zu Grunde, dann kann man bei jeder die Lagrange'sche Interpolationsformel § 37, Bd. I zur Bestimmung von g verwenden und erhält unter der entstehenden endlichen Anzahl von Functionen alle, welche bei einer Factorenzerlegung von f überhaupt in Frage kommen können. Mit jeder von ihnen muss dann die Division in f wirklich versucht werden; geht sie nicht auf, dann ist das g zu verwerfen; geht sie auf, dann hat man einen Divisor gefunden. Eine endliche Anzahl von ausführbaren Versuchen giebt demnach die Entscheidung über die Irreductibilität. Freilich steht es auch hier noch nicht fest, ob die Zerlegung in irreductible Theiler nur auf eine einzige Art möglich ist.

Als Beispiel behandeln wir die Function

$$f = z_1^3 z_2 + z_1^2(1 + z_2) + z_1(z_2^3 + z_2^2 + 1) + (z_2^2 + z_2); \quad (n = 4).$$

Hier ist freilich die geforderte Zubereitung der Function nicht ausgeführt. Diese verfolgte aber nur den Zweck, festzulegen, dass f keinen von z_1 unabhängigen Theiler besitze. Das ist hier von selbst klar, und deswegen kann jene Zubereitung bei Seite gelassen, und $\nu = 1$ gesetzt werden. Nun sei $z_1' = 0$, $z_1'' = 1$. Man hat dann

$$f(0, z_2) = z_2(z_2 + 1); \quad f(1, z_2) = (z_2^2 + z_2 + 2)(z_2 + 1),$$

und es ergeben sich hieraus als mögliche Werthe für

$$\begin{array}{llll} g(0, z_2) & \pm 1, & \pm z_2, & \pm (z_2 + 1); \\ g(1, z_2) & \pm 1, & \pm (z_2 + 1), & \pm (z_2^2 + z_2 + 2). \end{array}$$

Bei den Combinationen dieser beiden Werthesysteme giebt es $6 \cdot 6$ Möglichkeiten; es reicht aber offenbar aus, bei $g(0, z_2)$ die positiven Werthe allein zu betrachten, und dadurch reducirt sich die Anzahl auf $3 \cdot 6$ für

$$g(0, z_2)\frac{z_1 - 0}{1 - 0} + g(1, z_2)\frac{z_1 - 1}{0 - 1} = z_1[g(0, z_2) - g(1, z_2)] + g(1, z_2).$$

Von diesen 18 Möglichkeiten können diejenigen sofort beseitigt werden, bei denen $g(0, z_2) - g(1, z_2)$ kein Theiler von z_2, und diejenigen, bei denen $g(1, z_2)$ kein Theiler von $z_2^2 + z_2$ ist. Daher fällt $\pm(z_2^2 + z_2 + 2)$ ganz heraus; von den übrigen $3 \cdot 4$ kommen noch die beiden $g(0, z_2) = z_2 + 1$ und $g(1, z_2) = \pm(z_2 + 1)$ in Wegfall, weil aus ihnen g als Multiplum von $(z_2 + 1)$ hervorgehen würde, während doch f keinen von z_1 freien Theiler besitzt. Aus gleichem Grunde kann man $g(0, z_2) = 1$, $g(1, z_2) = 1$ unterdrücken. Es bleiben demgemäss schliesslich nur noch 9 Combinationen zurück; diese ergeben

$$\begin{gathered} -z_1 z_2 + z_2 + 1; \; -(z_2 + 2)z_1 + z_2 + 1; \; -(z_2 - 1)z_1 + z_2; \; -(z_2 + 1)z_1 + z_2; \\ z_1 + z_2; \quad -(2z_2 + 1)z_1 + z_2; \quad z_1 z_2 + 1; \quad -(z_2 + 2)z_1 + 1; \quad z_1 + 1, \end{gathered}$$

und nun überzeugt man sich leicht, dass $z_1 z_2 + 1$ die einzige Function ersten Grades von z_1 ist, welche in f aufgeht. Es wird

$$f = (z_1 z_2 + 1)(z_1^2 + z_1 + z_2^2 + z_2).$$

Unsere erste Methode wäre so vorgegangen. Für $z_1 = t$, $z_2 = t^2$ hätten wir

$$f = t^7 + 2t^5 + 2t^4 + 2t^3 + t;$$

diese Function kann auf folgende Art in Factoren zerlegt werden

$$f = t(t^3 + 1)(t^3 + 2t + 1).$$

Wir hätten nun die einzelnen Factoren, sowie die Producte aus je zwei unter ihnen in Functionen von z_1, z_2 zurück zu übersetzen. Dies ist freilich hier nicht auf eine einzige Art möglich, allein man überzeugt sich trotzdem leicht, dass

$$t^3 + 1 = z_1 z_2 + 1$$

ein Factor ist. Die letzte auftauchende Schwierigkeit rührt offenbar daher, dass q zu klein genommen worden ist.

§ 345. Wir kommen nun zur Aufsuchung des grössten gemeinsamen Theilers zweier Functionen $f(z_1, z_2, \cdots z_m)$ und $f_1(z_1, z_2, \cdots z_m)$

von den Dimensionen n und $(n - n_1)$. Beide sollen bereits so zubereitet sein, dass ihre Dimensionen mit ihren Graden nach z_1 übereinstimmen. Wir ordnen beide Functionen nach abnehmenden Potenzen von z_1, dividiren f durch f_1, indem wir beide als Functionen von z_1 behandeln, und erhalten $f = f_1 \cdot q_1 - f_2'$. Dabei ist q_1 eine ganze Function von $z_1, z_2, \cdots z_m$; es ist f_2' möglicherweise durch eine von z_1 unabhängige Function $\varphi_2(z_2, \cdots z_m)$ theilbar. Wir setzen, um diese zum Augenschein zu bringen, wenn sie vorhanden ist,

$$f = f_1 \cdot q_1 - f_2 \cdot \varphi_2,$$

wobei jetzt f_2 keinen gemeinsamen Theiler aller seiner Coefficienten in $z_2, \cdots z_m$ mehr besitzen soll. Der Grad von f_2 nach z_1 ist geringer als der von f_1, d. h. als $(n - n_1)$. Dividiren wir weiter f_1 durch f_2, beide Functionen als solche von z_1 betrachtet und nach fallenden Potenzen dieser Variablen entwickelt, so können in dem Quotienten und im Reste gebrochene Ausdrücke in $z_2, \cdots z_m$ erscheinen, und ausserdem kann möglicherweise aus den Coefficienten des Restes eine ganze Function in $z_2, \cdots z_m$ herausgezogen werden. Man kann demnach schreiben

$$\psi_1 \cdot f_1 = f_2 \cdot q_2 - f_3 \cdot \varphi_3,$$

wobei f_1, f_2, f_3, q_2 ganz in $z_1, z_2, \cdots z_m$, und ψ_1, φ_3 ganz in $z_2, \cdots z_m$ sind. ψ_1 und φ_3 können ohne gemeinsamen Theiler vorausgesetzt werden, weil ein gemeinsamer Theiler auch den Coefficienten von q angehören würde und fortgehoben werden könnte. f_3 ist in z_1 von geringerem Grade als f_2. So geht man weiter und erhält das Euklidsche Schema in der Gestalt

$$\begin{aligned}
f &= f_1 \cdot q_1 - f_2 \cdot \varphi_2 \\
\psi_1 \cdot f_1 &= f_2 \cdot q_2 - f_3 \cdot \varphi_3 \\
\psi_2 \cdot f_2 &= f_3 \cdot q_3 - f_4 \cdot \varphi_4 \\
&\cdots\cdots\cdots \\
\psi_{r-2} \cdot f_{r-2} &= f_{r-1} \cdot q_{r-1} - f_r \cdot \varphi_r \\
\psi_{r-1} \cdot f_{r-1} &= f_r \cdot q_r,
\end{aligned} \tag{5}$$

wobei wir allenfalls ein verschwindendes f_{r+1} noch hinzugefügt denken können. Haben wir die Division nämlich hinreichend weit fortgesetzt, so wird der Grad von z_1, der immer kleiner wird, ohne negativ werden zu können, einmal gleich Null werden, und die nächste Division nach z_1 wird aufgehen, wenn dies nicht schon früher eintritt.

Besitzen nun f und f_1 einen gemeinsamen Theiler, der nach unseren Vorbereitungen nicht von z_1 unabhängig sein kann, so hat ihn auch $f_2 \cdot \varphi_2$ und also nach § 342, (IV) auch f_2. Ebenso schliesst man, dass

ihn die Functionen $f_3, f_4, \cdots f_r$ besitzen. Umgekehrt ist f_r ein Theiler von $f_{r-1} \cdot \psi_{r-1}$, und da f_r keinen Theiler in $z_2, \cdots z_m$ besitzt, so theilt f_r wiederum (nach § 342, IV) auch f_{r-1}, u. s. w. Auf diesem Wege erkennt man, dass f_r auch f und f_1 theilt. Hierdurch ist der Begriff des grössten gemeinsamen Theilers unserer beiden zubereiteten Functionen f und f_1 festgelegt, und eine Methode zu seiner Aufsuchung gegeben. Es existirt, abgesehen von indifferenten Zahlenfactoren, nur eine unseren Forderungen genügende Function von $z_1, \cdots z_m$. Wir definiren: Eine ganze Function $T(z_1, \cdots z_m)$ heisst dann grösster gemeinsamer Theiler zweier zubereiteter Functionen f und f_1, wenn T beide Functionen theilt, aber nicht Divisor einer anderen Function derselben Eigenschaft ist. Unser Vorgehen zeigt dann: $T(z_1, \cdots z_m)$ ist bis auf indifferente Zahlenfactoren eindeutig bestimmt.

Diese Definition ist ebenso wie die Methode der Darstellung unseren zubereiteten Functionen angepasst. Beides kann aber leicht verallgemeinert werden. Sind nämlich g und g_1 willkürliche Functionen, so führt man sie durch eine lineare umkehrbare Substitution in die zubereiteten Formen f und f_1 über, sucht für diese den grössten gemeinsamen Theiler T und transformirt diesen durch die inverse Substitution in ein U, welches dann für g und g_1 die gleiche Eigenschaft hat wie T für f und f_1; denn auch U kann nicht in einer Function höherer Dimension aber gleicher Theilereigenschaft enthalten sein, weil dies sonst den gleichen Rückschluss auf T zuliesse.

Ist der grösste gemeinsame Theiler T von f und f_1 eine Constante, so heissen f und f_1 theilerfremd zu einander. Ist f_1 eine irreductible Function, so theilt sie entweder f oder sie ist zu f theilerfremd. Denn der grösste gemeinsame Theiler T muss als Theiler einer irreductiblen Function entweder gleich f_1 oder gleich einer Constanten sein.

Jede der in dem Schema (5) auftretenden Functionen $f_2, f_3, \cdots f_{r-1}, f_r$ lässt sich als lineare homogene Function von f und f_1 darstellen.

Es wird nämlich der Reihe nach aus (5) abgeleitet für ein beliebiges λ

$$\varphi_\lambda f_\lambda = f_{\lambda-1} \cdot q_{\lambda-1} - f_{\lambda-2} \cdot \psi_{\lambda-2},$$

$$(\varphi_\lambda \varphi_{\lambda-1}) f_\lambda = f_{\lambda-2} \cdot (q_{\lambda-1} q_{\lambda-2} - \varphi_{\lambda-1} \psi_{\lambda-2}) - f_{\lambda-3} \cdot q_{\lambda-1} \psi_{\lambda-3},$$

$$(\varphi_\lambda \varphi_{\lambda-1} \varphi_{\lambda-2}) f_\lambda = f_{\lambda-3} \cdot (q_{\lambda-1} q_{\lambda-2} q_{\lambda-3} - \varphi_{\lambda-1} \psi_{\lambda-2} q_{\lambda-3} - \varphi_{\lambda-2} \psi_{\lambda-3} q_{\lambda-1})$$
$$- f_{\lambda-4} (q_{\lambda-1} q_{\lambda-2} \psi_{\lambda-4} - \varphi_{\lambda-1} \psi_{\lambda-2} \psi_{\lambda-4}),$$

. . . .

so dass wir ansetzen können

$$(6)\qquad (\varphi_\lambda \varphi_{\lambda-1} \cdots \varphi_2) f_\lambda = P_{\lambda-1} f_1 - Q_{\lambda-1} f;$$

dabei sind die P und Q ganze Functionen der $z_1, \cdots z_m$, für welche die Formeln gelten

$$(7)\qquad \begin{array}{ll} P_{\lambda+1} = q_{\lambda+1} P_\lambda - \varphi_{\lambda+1} \psi_\lambda P_{\lambda-1}; & (P_0 = 1, \quad P_1 = q_1), \\ Q_{\lambda+1} = q_{\lambda+1} Q_\lambda - \varphi_{\lambda+1} \psi_\lambda Q_{\lambda-1}; & (Q_1 = 1, \quad Q_2 = q_2). \end{array}$$

Hieraus folgt dann

$$(7^a)\qquad \begin{array}{ll} P_2 = q_1 q_2 - \varphi_2 \psi_1; & P_3 = q_1 q_2 q_3 - \varphi_3 \psi_2 q_1 - \varphi_2 \psi_1 q_3; \cdots \\ Q_3 = q_2 q_3 - \varphi_3 \psi_2; & Q_4 = q_2 q_3 q_4 - \varphi_4 \psi_3 q_2 - \varphi_3 \psi_2 q_4; \cdots \end{array}$$

In dem Specialfalle $\lambda = r$ liefert (6) die Beziehung

$$(8)\qquad (\varphi_2 \varphi_3 \cdots \varphi_r) f_r = P_{r-1} \cdot f_1 - Q_{r-1} \cdot f.$$

Durch Combination der beiden Gleichungen (7) und durch wiederholte Anwendung der so gewonnenen Formel auf sich selbst erlangt man mit Hülfe von (7^a) das Resultat

$$(9)\qquad P_\lambda Q_{\lambda+1} - P_{\lambda+1} Q_\lambda = (\psi_1 \psi_2 \cdots \psi_\lambda) \cdot (\varphi_2 \varphi_3 \cdots \varphi_{\lambda+1}),$$

aus dem ersichtlich wird, dass die linke Seite von z_1 unabhängig bleibt. Combinirt man ferner (6) mit der durch Erhöhung von λ um 1 daraus entstehenden Gleichung und verwendet (9), so zeigt sich

$$(10)\qquad \begin{array}{l} (\psi_1 \psi_2 \cdots \psi_{\lambda-1}) f = P_\lambda \cdot f_\lambda - \varphi_{\lambda+1} P_{\lambda-1} \cdot f_{\lambda+1}, \\ (\psi_1 \psi_2 \cdots \psi_{\lambda-1}) f_1 = Q_\lambda \cdot f_\lambda - \varphi_{\lambda+1} Q_{\lambda-1} \cdot f_{\lambda+1}. \end{array}$$

Die Gradbestimmung der hier auftretenden Functionen nach z_1 entspricht durchaus derjenigen, welche § 64, Bd. I vorgetragen wurde, und die dortigen Resultate gelten auch hier.

$$[f] = n, \quad [f_1] = n - n_1, \cdots [f_\lambda] = n - n_\lambda, \quad \cdots [f_r] = n - n_r;$$
$$(0 \leqq n_1 < n_2 < \cdots < n_r \leqq n)$$
$$[q_1] = n_1, \quad [q_2] = n_2 - n_1, \cdots [q_\lambda] = n_\lambda - n_{\lambda-1}, \cdots [q_r] = n_r - n_{r-1};$$
$$[P_1] = n_1, \quad [P_2] = n_2, \quad \cdots \quad [P_\lambda] = n_\lambda, \quad \cdots \quad [P_r] = n_r;$$
$$[Q_1] = 0, \quad [Q_2] = n_2 - n_1, \cdots [Q_\lambda] = n_\lambda - n_1, \quad \cdots \quad [Q_r] = n_r - n_1.$$

In (8) ist demnach der Grad von P_{r-1} nach z_1 gleich n_{r-1}, d. h. $< n_r \leqq n$, also höchstens gleich $(n - 1)$; und der Grad von $Q_{r-1} = (n_{r-1} - n_1)$, d. h. $< (n - n_1) - 1$. Das zeigt: Bei der Darstellung des grössten gemeinsamen Theilers von f und f_1 durch (8) genügt für P_{r-1} eine Function, deren Grad in z_1 kleiner als der von f ist, und für Q_{r-1} eine solche, deren Grad in z_1 kleiner als der von f_1 ist.

§ 346. (VI) Sind $f_1(z_1, z_2, \cdots z_m)$ und $g(z_1, z_2, \cdots z_m)$ theilerfremd zu einander, und ist das Product $f_1(z_1, \cdots z_m) \cdot f_2(z_1, \cdots z_m)$ durch g theilbar, dann ist f_2 durch g theilbar.

Wir nehmen, was den Charakter der Theilbarkeit ja nicht beeinflusst, f_1, f_2 und g so vorbereitet an, dass ihre Grade in z_1 mit ihren Dimensionen übereinstimmen. Da f_1 und g theilerfremd sind, so kann man nach (8)

$$f_1 \cdot P + g \cdot Q = \Phi(z_2, \cdots z_m)$$

setzen, woraus dann durch Multiplication mit f_2

$$(f_1 f_2) P + g(f_2 Q) = \Phi \cdot f_2$$

folgt; nach der Voraussetzung ist $f_1 f_2$ und also die linke Seite durch g theilbar; also auch $\Phi \cdot f_2$ und nach § 343, (IV) auch f_2.

Hierdurch haben wir den Satz für m Veränderliche bewiesen, welcher in § 342 für $(m - 1)$ Veränderliche als richtig angenommen wurde; und damit ist die Beweisführung geschlossen.

(VII) Ist das Product $f_1 \cdot f_2$ durch eine irreductible Function g theilbar, so ist mindestens einer der Factoren f_1 oder f_2 durch g theilbar. Denn da g irreductibel ist, so muss es entweder f_1 theilen, oder zu f_1 theilerfremd sein. Der zweite Fall erledigt sich dann sofort durch Satz (VI).

(VIII) Eine Function $f(z_1, z_2, \cdots z_m)$ von m Variablen ist nur auf Eine Art in irreductible Factoren zerlegbar. Der Beweis ist dem für $(m - 1)$ Variable gegebenen durchaus entsprechend, so dass er hier nicht behandelt zu werden braucht.

(IX) Wenn $f(z_1, \cdots z_m)$ für alle Werthsysteme verschwindet, welche eine irreductible Function $g(z_1, \cdots z_m)$ zu Null machen, dann ist f durch g theilbar.

Wäre das nicht der Fall, so würden f und g theilerfremd sein, und man könnte die Gleichung

$$P \cdot f + Q \cdot g = \Phi(z_2, \cdots z_m)$$

aufstellen, in welcher Φ nicht identisch Null ist. Wir können daher $z_2 = \zeta_2, \cdots z_m = \zeta_m$ setzen, wo die ζ so gewählt sind, dass sie Φ nicht gleich Null machen. Zu diesem Systeme bestimmen wir ein $z_1 = \zeta_1$ durch die Forderung $g(z_1, \zeta_2, \cdots \zeta_m) = 0$. Dies ist natürlich nur möglich, wenn z_1 aus $g(z_1, \zeta_2, \cdots \zeta_m)$ nicht herausfällt. Wir ordnen daher g nach Potenzen von z_1

$$g = \psi_0 z_1^{r_1} + \psi_1 z_1^{r_1 - \alpha} + \psi_2 z_1^{r_1 - \beta} + \cdots,$$

wobei die ψ nur die nicht identisch verschwindenden Coefficienten bezeichnen sollen, und beschränken die Wahl der $\zeta_2, \cdots \zeta_m$ durch die

Forderung, dass $\psi_0 \cdot \Phi \neq 0$ sei. Dann kann man auch ein passendes $z_1 = \zeta_1$ finden. Für dieses System der ζ müsste der Voraussetzung gemäss auch f verschwinden; das kann aber nicht sein, weil $\Phi \neq 0$ ist. Es muss deshalb g ein Theiler von f sein.

(X) Wenn $f(z_1, \cdots z_m)$ für alle Werthsysteme verschwindet, welche eine Function $g(z_1, \cdots z_m)$ zu Null machen, dann ist f durch jeden der verschiedenen irreductiblen Factoren von g theilbar, und eine passende Potenz von f durch g selbst. Das folgt sofort aus dem vorigen Satze.

(XI) Besteht kein Werthsystem $\zeta_1, \zeta_2, \cdots \zeta_m$, welches die beiden Gleichungen

$$(11) \qquad f_1(z_1, z_2, \cdots z_m) = 0, \qquad f_2(z_1, z_2, \cdots z_m) = 0$$

gleichzeitig befriedigt, dann giebt es zwei ganze Functionen $P(z_1, z_2, \cdots z_m)$ und $Q(z_1, z_2, \cdots z_m)$, für welche die Relation

$$(12) \qquad f_1 \cdot P + f_2 \cdot Q = 1$$

besteht. Umgekehrt: gilt (12), dann giebt es kein Werthsystem $\zeta_1, \zeta_2, \cdots \zeta_m$, welches (11) befriedigt.

Zunächst ist es klar, dass im ersten Falle f_1 und f_2 theilerfremd sein müssen, sodass man also zwei Functionen P und Q so bestimmen kann, dass

$$f_1 \cdot P + f_2 \cdot Q = \Phi(z_2, \cdots z_m)$$

wird. Kann man nun $\zeta_2, \cdots \zeta_m$ gemäss der Bedingung $\Phi(\zeta_2, \cdots \zeta_m) = 0$ wählen, so entsteht

$$f_1(z_1, \zeta_2, \cdots \zeta_m) P(z_1, \zeta_2, \cdots \zeta_m) = -f_2(z_1, \zeta_2, \cdots \zeta_m) Q(z_1, \zeta_2, \cdots \zeta_m).$$

Nach § 345 ist $[P] < [f_2]$ bezogen auf z_1. Folglich hat $f_1(z_1, \zeta_2, \cdots)$ mit $f_2(z_1, \zeta_2, \cdots)$ einen Factor gemein; aus ihm kann man $z_1 = \zeta_1$ so bestimmen, dass (11) befriedigt wird. Das widerspricht aber der Voraussetzung. Also ist Φ eine Constante. Dividirt man durch sie, so kommt man auf (12). — Die Umkehrung bedarf keines Beweises.

(XII) Ist $T(z_1, z_2, \cdots z_m)$ der grösste gemeinsame Theiler, der nach § 340 vorbereiteten Functionen $f_1(z_1, \cdots z_m)$, $f_2(z_1, \cdots z_m)$, $f_3(z_1, \cdots z_m), \cdots$, dann giebt es ganze Functionen $P_1(z_1, \cdots z_m)$, $P_2(z_1, \cdots z_m)$, $P_3(z_1, \cdots z_m), \cdots$; $\Phi(z_2, \cdots z_m)$, welche die Gleichung

$$(13) \qquad f_1 P_1 + f_2 P_2 + f_3 P_3 + \cdots = T \cdot \Phi$$

befriedigen. — Die Definition des grössten gemeinsamen Theilers beliebig vieler Functionen ist klar. Nun giebt es nach (8) für den grössten gemeinsamen Theiler $T_{1,2}$ von f_1 und f_2 eine Gleichung von der Form

$$f_1 P_{1,2} + f_2 Q_{1,2} = T_{1,2} \cdot \Phi_{1,2};$$

ebenso für den grössten gemeinsamen Theiler $T_{1,2,3}$ von $T_{1,2}$ und f_3 eine Gleichung von der Form

$$T_{1,2} \cdot P_{1,2,3} + f_3 \cdot Q_{1,2,3} = T_{1,2,3} \cdot \Phi_{1,2,3}.$$

Daraus ergiebt sich

$$f_1 \cdot (P_{1,2} P_{1,2,3}) + f_2 \cdot (Q_{1,2} P_{1,2,3}) + f_3 \cdot (\Phi_{1,2} Q_{1,2,3}) = T_{1,2,3} \cdot (\Phi_{1,2} \Phi_{1,2,3}).$$

Dies entspricht der Behauptung im Falle dreier Functionen. — In gleicher Art führt man den Beweis für mehr Functionen.

(XIII) Wenn es für jedes System $\zeta_2, \zeta_3, \cdots \zeta_m$ einen Werth ζ_1 giebt, derart, dass $z_1 = \zeta_1, z_2 = \zeta_2, \cdots z_m = \zeta_m$ die Gleichungen

$$(11) \qquad f_1(z_1, z_2, \cdots z_m) = 0, \qquad f_2(z_1, z_2, \cdots z_m) = 0$$

befriedigt, dann haben f_1 und f_2 einen gemeinsamen Theiler. — Denn gesetzt, das wäre nicht der Fall, dann könnte man ansetzen

$$f_1 \cdot P_1 + f_2 \cdot P_2 = \Phi(z_2, \cdots z_m).$$

Wählen wir nun $\zeta_2, \cdots \zeta_m$ so, dass $\Phi(\zeta_2, \cdots \zeta_m) \neq 0$, und dann ζ_1 der Voraussetzung gemäss, so dass (11) durch $\zeta_1, \cdots \zeta_m$ befriedigt wird, dann stossen wir auf einen Widerspruch. Es muss also Φ für jedes System $\zeta_2, \cdots \zeta_k$ verschwinden, d. h. nach dem ersten Paragraphen dieser Vorlesung identisch gleich Null sein. Dann folgt, wie in (XI), dass f_1 und f_2 einen gemeinsamen Teiler besitzen.

Zweiunddreissigste Vorlesung.

Wurzeln einer Gleichung und eines Gleichungssystems mehrerer Variablen.

§ 347. Wir haben im Laufe der beiden letzten Vorlesungen mitunter den Satz benutzt, dass es Werthsysteme giebt, welche eine ganze Function von m Veränderlichen $f(z_1, z_2, \cdots z_m)$ zu Null macht. Das bedurfte auch keines besonderen Beweises; denn es ist klar, dass man $z_2, z_3, \cdots z_m$ beliebig gleich den Constanten $\zeta_2, \zeta_3, \cdots \zeta_m$ annehmen und dann die Gleichung $f(z_1, \zeta_2, \cdots \zeta_m) = 0$ nach z_1 lösen kann. Hierbei könnte freilich Folgendes eintreten: es könnten in

$$(1)\ f(z_1, z_2, \cdots z_m) = \varphi_0(z_2, \cdots z_m) z_1^{r_1} + \varphi_1(z_2, \cdots z_m) z_1^{r_1 - 1} + \cdots + \varphi_{r_1}(z_2, \cdots z_m)$$

alle Coefficienten φ für $(z_2, \cdots z_m) = (\zeta_2, \cdots \zeta_m)$ verschwinden. Dann genügt eben jedes Werthsystem $(z_1, \zeta_2, \cdots \zeta_m)$ der Forderung. Es

könnte aber auch $\varphi_0, \varphi_1, \cdots \varphi_{r_1-1}$ verschwinden, während φ_{r_1} von Null verschieden bleibt. Um das zu vermeiden, reicht es aus, $\varphi_{r_1}(z_2, \cdots z_m) = 0$ zu machen, und das reducirt unsere Forderung von m Variablen auf $(m - 1)$. Da sie für $m = 1$ erfüllbar ist, so gilt also der Satz allgemein, dass man ein System finden kann, für welches f verschwindet. Die aufgeworfene Schwierigkeit lässt sich aber auch noch in anderer Weise überwinden, wie wir im § 349 zeigen werden.

§ 348. Ein System von Werten $z_1 = \zeta_1, z_2 = \zeta_2, \cdots z_m = \zeta_m$, welches die Gleichung

$$f(z_1, z_2, \cdots z_m) = 0 \tag{2}$$

befriedigt, soll eine Wurzel der Gleichung (2) heissen; ebenso ein System, welches die Gleichungen

$$f_\alpha(z_1, z_2, \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots q) \tag{3}$$

befriedigt, eine Wurzel des Gleichungssystems (3). Wir werden uns auch die Bezeichnung „Wurzel der Function f“ oder „Wurzel des Functionensystems f_α“ erlauben, da durch diese, freilich etwas lässige Benennung doch keinerlei Irrthümer entstehen können.

Es kann auf den ersten Blick befremdlich erscheinen, ein solches System $\zeta_1, \zeta_2, \cdots \zeta_m$ von Werten als „eine Wurzel“ zu bezeichnen. Man möchte geneigt sein, bei zwei Gleichungen etwa von „Wurzel-Paaren“, bei dreien von „Wurzel-Tripeln“ u. s. f. zu sprechen. Das wäre aber durchaus unangebracht. Denn ζ_1, ζ_2 ist nicht ein Paar von Wurzeln einer Gleichung $f(z_1, z_2) = 0$, weil ζ_1 und ζ_2 für sich keine Wurzeln sind; sie stellen erst in ihrer Verbindung ein Werthsystem dar, welches die vorgelegte Gleichung befriedigt. Es ist deshalb nothwendig, bei der Wahl eines Namens darauf zu achten, dass das System der ζ als Ganzes in die Bezeichnung eintritt. Passend würde auch die geometrische Bezeichnung „Wurzelpunkt“ sein, wobei dann $\zeta_1, \zeta_2, \cdots \zeta_m$ als seine Coordinaten aufgefasst werden könnten; es soll das auch mitunter geschehen. Die einfache Uebertragung der Nomenclatur „Wurzel“ von $f(z) = 0$ auf (2), (3) hat um so weniger Bedenken, als ja auch schon bei $f(z) = 0$ der Name nur uneigentlich aufgefasst werden darf, sobald es sich wenigstens um andere als um binomische Gleichungen $f(z) = 0$ handelt.

§ 349. Wir haben schon bemerkt, dass bei einer Function (1) von $m > 1$ Variablen ein Fall eintreten kann, der bei Einer Variablen nicht möglich war; es kann der Coefficient φ_0 der höchsten Potenz $z_1^{r_1}$ einer der Variablen z_1 bei gewissen Werten $z_2 = \zeta_2, \cdots z_m = \zeta_m$ verschwinden.

Wenn wir nun statt z_1 eine neue Variable $y_1 = \frac{1}{z_1}$ einführen, dann geht (1) in

$$\varphi_{r_1}(z_2, \cdots z_m) y_1^{r_1} + \varphi_{r_1-1}(z_2, \cdots z_m) y_1^{r_1-1} + \cdots + \varphi_1(z_2, \cdots z_m) y_1 + \varphi_0(z_2, \cdots z_m) = 0$$

über, und man sieht, dass diese Gleichung in y_1 für $z_2 = \zeta_2, \cdots z_m = \zeta_m$ die Wurzel $y_1 = 0$ besitzt. Wir dürfen dies so aussprechen, dass wir sagen: (1) besitzt für $\zeta_2, \cdots \zeta_m$ eine unendlich grosse Wurzel für z_1, also $z_1 = \infty$.

Wendet man aber auf (1) die vorbereitende Substitution des § 340 an, so erscheint (1) in einer Form, in welcher die Coefficienten von $y_1^n, y_2^n, \cdots$ sämmtlich Constanten $\neq$ werden. Dadurch ist die eben besprochene Eventualität ausgeschaltet. Es fragt sich aber, was hier aus der unendlich grossen Wurzel geworden ist. Die Betrachtung der Formel (4), § 340 zeigt, dass eine Wurzel $y_1 = \infty$, $y_2 = \infty$, $\cdots y_m = \infty$ vorhanden sein muss.

Wir denken uns dies folgendermassen: Wir ordnen die transformirte Function in $y_1, y_2, \cdots y_m$ nach den Dimensionen ihrer Glieder

$$u_n(y_1, \cdots y_m) + u_{n-1}(y_1, \cdots y_m) + \cdots + u_0(y_1, \cdots y_m) = 0,$$

wobei u_α alle Glieder der α^{ten} Dimension enthalten soll, und setzen nun

$$y_1 = x_1 t, \quad y_2 = x_2 t, \quad \cdots y_m = x_m t$$

unter der Annahme $x_m = 1$. Dann erhalten wir

$$u_n(x_1, \cdots x_{m-1}, 1) \cdot t^n + u_{n-1}(x_1, \cdots x_{m-1}, 1) \cdot t^{n-1} + \cdots + u_0(x_1, \cdots x_{m-1}, 1) = 0,$$

und nach dem soeben Besprochenen wird für jedes System $x_1 = \xi_1$, $\cdots x_{m-1} = \xi_{m-1}$, welches $u_n(\xi_1, \cdots \xi_{m-1}, 1) = 0$ macht, $t = \infty$ eine Wurzel der Gleichung in t sein. Wir können also

$$y_1 = \xi_1 t, \quad y_2 = \xi_2 t, \quad \cdots y_{m-1} = \xi_{m-1} t, \quad y_m = t \qquad (\lim t = \infty)$$

als Wurzel der Gleichung in $y_1, \cdots y_m$ ansehen.

Bei Gleichungen mit mehreren Variablen ist zwischen endlichen und unendlichen Lösungen scharf zu unterscheiden. Aehnliches findet bei Gleichungssystemen statt; wir werden auf Theoreme stossen, die nur dann gültig sind, wenn das Gleichungssystem, auf welches sie sich beziehen, nur endliche Wurzeln hat. In welchem Sinne bei einem Systeme (3) von unendlich grossen Wurzeln gesprochen werden kann, ist nach dem soeben für eine Gleichung Dargelegten von selbst klar.

§ 350. Bei einer Gleichung mit einer Variablen $f(z) = 0$ folgte aus der Existenz einer Wurzel ζ die Beziehung

$$f(z) = (z - \zeta)\, g(z, \zeta),$$

wobei $g(z, \zeta)$ eine ganze Function von z und ζ war, deren Grad in z um 1 geringer wurde, als der Grad von $f(z)$.

Ist $(\zeta_1, \zeta_2, \cdots \zeta_m)$ eine Wurzel von (2), so folgt

$$(4)\quad f(z_1, \cdots z_m) = (z_1 - \zeta_1) \cdot g_1 + (z_2 - \zeta_2) \cdot g_2 + \cdots + (z_m - \zeta_m) \cdot g_m,$$

wobei die $g_1, g_2, \cdots g_m$ Functionen der $z_1, z_2, \cdots z_m, \zeta_1, \zeta_2, \cdots \zeta_m$ sind. Das ist leicht einzusehen; denn man hat ja

$$\begin{aligned} f(z_1, \cdots z_m) = & [f(z_1, z_2, \cdots z_m) - f(\zeta_1, z_2, \cdots z_m)] \\ & + [f(\zeta_1, z_2, \cdots z_m) - f(\zeta_1, \zeta_2, \cdots z_m)] \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + [f(\zeta_1, \cdots \zeta_{m-1}, z_m) - f(\zeta_1, \cdots \zeta_{m-1}, \zeta_m)] \\ & + f(\zeta_1, \cdots \zeta_{m-1}, \zeta_m). \end{aligned}$$

Hier ist jede der eckigen Klammern durch eine der Differenzen $(z_\alpha - \zeta_\alpha)$ theilbar, und der letzte Summand verschwindet. Damit ist die Gültigkeit von (4) dargethan. Zugleich sieht man, dass die Darstellung (4) auf unendliche viele Arten vor sich gehen kann. (Vgl. § 463 ff.)

Die Bedeutung von (4) liegt aber in anderer Richtung, als bei der entsprechenden Formel für eine Variable. Wenn in diesem Falle ζ' eine zweite Wurzel von $f(z) = 0$ bedeutete, dann folgte weiter

$$f(z) = (z - \zeta)(z - \zeta')\, h(z, \zeta, \zeta')$$

u. s. f., so dass eine Zerfällung von f in lineare Factoren möglich wurde.

Bei unserer jetzigen Formel versagen die entsprechenden Schlüsse. Ist $(\zeta_1', \zeta_2', \cdots \zeta_m')$ eine zweite Wurzel von (2), so ist zwar

$$(\zeta_1' - \zeta_1)\, g_1(\zeta, \zeta') + (\zeta_2' - \zeta_2)\, g_2(\zeta, \zeta') + \cdots = 0,$$

wobei die g Functionen aller Coordinaten $\zeta_\alpha, \zeta_\alpha'$ sind, aber eine ähnliche Reduction wie oben tritt nicht ein.

Man könnte versuchen, auf folgende Weise vorzugehen. Wir setzen

$$z_1 - \zeta_1 = u_1, \quad z_2 - \zeta_2 = u_1 u_2, \quad z_3 - \zeta_3 = u_1 u_3, \quad \cdots \quad z_m - \zeta_m = u_1 u_m,$$

und führen die neuen Unbekannten in (4) ein. Dann kann u_1 aus allen Summanden herausgesetzt werden, derart, dass sich jetzt die Form ergiebt $f = u_1 \cdot g(u_1, u_2, \cdots u_m)$, und wenn $(\zeta_1', \zeta_2', \cdots \zeta_m')$ eine neue Wurzel von (2) bedeutet, bei der etwa $\zeta_1' \neq \zeta_1$ sein soll, so muss für

$$u_1 = \zeta_1' - \zeta_1, \quad u_1 u_2 = \zeta_2' - \zeta_2, \quad u_1 u_3 = \zeta_3' - \zeta_3, \quad \cdots$$

die Function g verschwinden, so dass in ähnlicher Weise aus ihr ein Factor abgesondert werden könnte. Allein man überzeugt sich leicht, dass damit kein Fortschritt verbunden ist, weil man aus dem Bereiche ganzer Functionen in denjenigen gebrochener Functionen gelangt.

Wir wollen dies an dem einfachen Beispiel der Function $f = z_1^2 - z_2^2$ durchführen. Für $z_1 - a = u_1$, $z_2 - a = u_1 u_2$ erhält man

$$f = u_1(1 - u_2)(u_1 + u_1 u_2 + 2a);$$

benutzt man nun die Wurzel $(z_1, z_2) = (b, -b)$, so werden als Wurzelwerthe der u folgen $(u_1, u_2) = \left(b - a, \frac{a+b}{a-b}\right)$. Es ist also

$$v_1 = u_1 + (a - b), \quad v_1 v_2 = u_2 - \frac{a+b}{a-b}$$

einzuführen. Dadurch entsteht

$$f = u_1(1 - u_2)v_1\left(\frac{2a}{a-b} + (b - a)v_2 + v_1 v_2\right).$$

Nun ergiebt sich sofort, dass für jede Wurzel $(z_1, z_2) = (c, c)$ der zweite Factor verschwindet, und für $(z_1, z_2) = (c, -c)$ der letzte Factor, aber eine Einsicht in das Wesen der Function wird dadurch nicht gewonnen.

§ 351. Aus (4) können wir aber eine ungezwungene Definition für vielfache Wurzeln einer Gleichung (2) ziehen. Sind auch $g_1 = 0$, $g_2 = 0, \cdots g_m = 0$ in (4) durch $\zeta_1, \zeta_2, \cdots \zeta_m$ befriedigt, d. h. ist auch

$$(5) \qquad f(z_1, \cdots z_m) = \Pi(z_\alpha - \zeta_\alpha)(z_\beta - \zeta_\beta)g_{\alpha,\beta},$$

wobei α, β alle gleichen wie ungleichen Combinationen zweier Zahlen $1, 2, \cdots m$ sein sollen, dann nennen wir $(\zeta_1, \zeta_2, \cdots \zeta_m)$ eine Doppelwurzel von (2). Ebenso mag allgemein $(\zeta_1, \zeta_2, \cdots \zeta_m)$ eine ϱ-fache Wurzel oder eine Wurzel von der Multiplicität ϱ genannt werden, wenn f als homogene Function ϱ^{ter} Ordnung der m Grössen $(z_1 - \zeta_1)$, $\cdots (z_m - \zeta_m)$ mit Coefficienten darstellbar ist, welche ganze Functionen der $z_1, z_2, \cdots z_m, \zeta_1, \zeta_2, \cdots \zeta_m$ sind.

Wir können das Gleiche auch so aussprechen, dass für eine Doppelwurzel nicht nur die Function f, sondern auch ihre sämmtlichen ersten Ableitungen, nämlich $\frac{\partial f}{\partial z_1}, \frac{\partial f}{\partial z_2}, \cdots \frac{\partial f}{\partial z_m}$ verschwinden; für eine dreifache Wurzel ausserdem noch $\frac{\partial^2 f}{\partial z_1^2}, \frac{\partial^2 f}{\partial z_1 \partial z_2}, \cdots \frac{\partial^2 f}{\partial z_m^2}$, u. s. w., so dass eine ϱ-fache Wurzel dadurch charakterisirt ist, dass für sie die Function selber und alle ihre Ableitungen bis zu denen der $(\varrho - 1)^{\text{ten}}$ Ordnung inclusive verschwinden.

Was unter mehrfachen Wurzeln eines Gleichungssystems zu verstehen ist, und wie solche mehrfachen Wurzeln ihrer Multiplicität nach zu bestimmen sind, lässt sich an dieser Stelle noch nicht auseinandersetzen.

§ 352. Entsprechend der in § 37 Bd. I behandelten Frage gehen wir jetzt dazu über, die Bestimmung einer Function $f(z_1, \cdots z_m)$ der

n^{ten} Dimension dadurch zu liefern, dass für eine ausreichende Zahl ϱ von Werthsystemen für $(z_1, \cdots z_m)$, nämlich für

$$(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}), \quad \text{die Werte} \quad f(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}) = f^{(\varrho)}$$

vorgeschrieben werden. Aus § 329 folgt für die Anzahl der Coefficienten, welche in f eingehen, der Wert $N(n, m)$; so gross muss ϱ angenommen werden. Wir erhalten dann ebenso viele lineare Gleichungen von der Form

$$\sum c_{\varkappa,\lambda,\mu,\ldots} \zeta_{1\alpha}^{\varkappa} \zeta_{2\alpha}^{\lambda} \zeta_{3\alpha}^{\mu} \cdots - f^{(\alpha)} = 0 \qquad (\alpha = 1, 2, \cdots \varrho)$$

für die ϱ Unbekannten $c_{\varkappa,\lambda,\mu,\ldots}$; verbinden wir mit diesen noch die Gleichung

$$\sum c_{\varkappa,\lambda,\mu,\ldots} z_1^{\varkappa} z_2^{\lambda} z_3^{\mu} \cdots - f = 0,$$

so können wir aus unserem Systeme sofort sämmtliche c eliminiren und erhalten als Resultat den gesuchten Ausdruck der Function $f(z_1, \cdots z_m)$. Dabei ergiebt sich eine Determinante der Ordnung $(\varrho + 1)$

$$(6) \qquad \begin{vmatrix} f, & 1, & z_1, & z_2, & \cdots z_1^{\varkappa} z_2^{\lambda} z_3^{\mu} & \cdots, & \cdots \\ f^{(1)}, & 1, & \zeta_{11}, & \zeta_{21}, & \cdots \zeta_{11}^{\varkappa} \zeta_{21}^{\lambda} \zeta_{31}^{\mu} & \cdots, & \cdots \\ f^{(2)}, & 1, & \zeta_{12}, & \zeta_{22}, & \cdots \zeta_{12}^{\varkappa} \zeta_{22}^{\lambda} \zeta_{32}^{\mu} & \cdots, & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} = 0.$$

Diese Form liefert f stets in einer ganz bestimmten Art, sobald die Subdeterminante

$$\varDelta_0 = \begin{vmatrix} 1, & \zeta_{11}, & \zeta_{21}, & \cdots \zeta_{11}^{\varkappa} \zeta_{21}^{\lambda} \zeta_{31}^{\mu} & \cdots, & \cdots \\ 1, & \zeta_{12}, & \zeta_{22}, & \cdots \zeta_{12}^{\varkappa} \zeta_{22}^{\lambda} \zeta_{32}^{\mu} & \cdots, & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} \neq 0$$

ist. Es möge (6), nach den Elementen der ersten Spalte entwickelt,

$$f\varDelta_0 - f^{(1)}\varDelta_1 - f^{(2)}\varDelta_2 - \cdots - f^{(\varrho)}\varDelta_\varrho = 0$$

geben, dann ist das Analogon zur Lagrange'schen Interpolationsformel in der Formel

$$(7) \quad f(z_1, \cdots z_m) = f^{(1)} \frac{\varDelta_1}{\varDelta_0} + f^{(2)} \frac{\varDelta_2}{\varDelta_0} + \cdots + f^{(\varrho)} \frac{\varDelta_\varrho}{\varDelta_0} \qquad (\varrho = N(n, m))$$

enthalten. Dabei ist $\varDelta_0$ von den Variablen $z_1, \cdots z_m$ frei. Die Analogie zeigt sich auch darin, dass $\varDelta_\alpha$ für alle Systeme $\zeta_1, \cdots \zeta_m$ mit Ausnahme von $\zeta_{1\alpha}, \cdots \zeta_{m\alpha}$ verschwindet und für dieses System $\zeta_{1\alpha}, \cdots \zeta_{m\alpha}$ gleich $\varDelta_0$ wird; also verhält sich die Bildung hier ganz ähnlich wie die früher für eine einzige Variable gegebene. Hier ist noch der Nachweis dafür erforderlich, dass $\varDelta_0$ nicht identisch, d. h. für jede Wahl des ζ verschwindet. Um diesen zu liefern, wenden wir zunächst die Kronecker'sche Transformation

$$\zeta_{1\alpha} = t_\alpha, \quad \zeta_{2\alpha} = t_\alpha^q, \quad \zeta_{3\alpha} = t_\alpha^{q^2}, \cdots$$

an, und hätten zu zeigen, dass die Determinante

$$| 1, \; t_\alpha, \; t_\alpha^q, \; t_\alpha^{q+1}, \cdots t_\alpha^{mq^2+pq+r}, \cdots | \quad (\alpha = 1, 2, \cdots \varrho)$$

nicht verschwindet, falls q so hoch gewählt ist, dass alle Potenzproducte in $\varDelta_0$ verschiedene Exponenten von t bekommen. Die letzte Determinante ist eine Function von t_1 mit endlicher Gradzahl; sie kann nicht identisch Null sein, wenn nicht auch ihr absolutes Glied identisch verschwindet. Bei dieser aber bleibt, falls $t_2 \cdot t_3 \cdots t_\varrho$ herausgesetzt wird, eine Determinante ähnlicher Bildung von geringerer Ordnung zurück. Da nun der Satz für zwei Variable klar ist, so ist er allgemein richtig.

Setzt man nun in (6) oder in (7) alle $f^{(\alpha)} = 0$, so folgt, dass, wenn nicht besondere Beziehungen zwischen den $(\zeta_{1\alpha}, \zeta_{2\alpha}, \cdots \zeta_{m\alpha})$ bestehen, die Function $f(z_1, \cdots z_m)$ verschwindet; d. h. zwischen $\varrho = N(n, m)$ Wurzeln der Gleichung $f = 0$ findet die Relation $\varDelta_0 = 0$ statt. Stimmen zwei Functionen n^{ter} Dimension von m Variablen für $\varrho = N(n, m)$ Werthsysteme überein, zwischen denen die Relation $\varDelta_0 = 0$ nicht stattfindet, dann sind sie identisch.

Setzt man in (6) alle $f^{(\alpha)}$ mit Ausnahme des letzten $= 0$, und dieses $= (-1)^{\varrho-1} \cdot c$, so entsteht

$$(8) \qquad f(z_1, \cdots z_m) \cdot \varDelta_0 = c \begin{vmatrix} 1, & z_1, & z_2, & \cdots \\ 1, & \zeta_{11}, & \zeta_{21}, & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \zeta_{1,\varrho-1}, & \zeta_{2,\varrho-1} & \cdots \end{vmatrix},$$

somit ist hierdurch f bis auf einen constanten Factor durch $(\varrho - 1)$ seiner Wurzeln bestimmt und damit die in § 350 gesuchte Analogie zu den Functionen einer Veränderlichen gefunden, soweit eine solche vorhanden war.

§ 353. Wir wollen annehmen, was im Wesen der folgenden Betrachtung nichts ändert, dass die Function f so vorbereitet sei, dass ihr Grad in z_1 gleich ihrer Dimension n geworden ist; dabei wird der Coefficient von z_1^n eine Constante, die gleich 1 gesetzt werden mag. Es soll dann die Gleichung

$$f \equiv z_1^n + \varphi_1(z_2, \cdots z_m) z_1^{n-1} + \cdots + \varphi_{n-1}(z_2, \cdots z_m) z_1 + \varphi_n(z_2, \cdots z_m) = 0$$

als Gleichung für z_1 aufgefasst zu dem Werthsystem $z_2 = \zeta_2, \cdots z_m = \zeta_m$ die α-fache Wurzel $z_1 = 0$ besitzen. Hierfür ist charakteristisch das Bestehen der Gleichungen

$$\varphi_n(\zeta_2, \cdots \zeta_m) = 0, \quad \varphi_{n-1}(\zeta_2, \cdots \zeta_m) = 0, \quad \cdots \quad \varphi_{n-\alpha+1}(\zeta_2, \cdots \zeta_m) = 0$$

und der Ungleichung

$$\varphi_{n-\alpha}(\zeta_2, \cdots \zeta_m) \neq 0.$$

Wir wollen nun den $z_2, z_3, \cdots z_m$ Incremente $\delta_2, \delta_3, \cdots \delta_m$ erteilen, welche so klein angenommen werden können, dass alle

$$\varphi_{n-k}(\zeta_2 + \delta_2, \cdots \zeta_m + \delta_m) \qquad (\varkappa = 0, 1, \cdots \alpha - 1)$$

ihrem absoluten Werthe nach unter einer beliebig kleinen Grenze bleiben, während die Function

$$\varphi_{n-\alpha}(\zeta_2 + \delta_2, \cdots \zeta_m + \delta_m)$$

um eine angebbare endliche Grösse von der Null entfernt bleibt. Das Product sämmtlicher Wurzeln $\zeta_{11}, \zeta_{12}, \cdots \zeta_{1m}$ der Gleichung in z_1

$$f(z_1, \zeta_2 + \delta_2, \cdots \zeta_n + \delta_n) = 0,$$

ist dann $\pm \varphi_n(\zeta_2 + \delta_2, \cdots)$ und daher beliebig klein. Deswegen muss mindestens eins der $|\zeta_1|$ selbst hinreichend klein werden, etwa $|\zeta_{11}|$. Ferner ist die Summe der Producte von je $(n-1)$ der Wurzeln ζ_1 gleich $\mp \varphi_{n-1}(\zeta_2 + \delta_2, \cdots)$ und somit auch beliebig klein. Nur einer der Summanden, nämlich $\zeta_{12}\zeta_{13}\cdots\zeta_{1n}$, enthält ζ_{11} nicht; deswegen ist auch noch ein zweites $|\zeta_1|$, etwa $|\zeta_{12}|$, hinreichend klein. In dieser Weise kann man fortgehen und kommt zu der Einsicht, dass genau α der absoluten Werthe der Wurzeln ζ_1 hinreichend klein werden, d. h. dass die Wurzeln den früheren Werten 0 hinreichend benachbart sind. Diese ändern sich also zugleich mit $z_2, \cdots z_m$ in stetiger Weise. Die Beschränkung auf $z_1 = 0$ kann durch Einführung von $(z_1 - a)$ statt z_1 aufgehoben werden; und was für die α Wurzeln $z = 0$ galt, gilt demgemäss allgemein: Die Wurzeln $z_1 = \zeta_{11}, \zeta_{12}, \cdots$ von $f = 0$ ändern sich stetig zugleich mit $z_2, z_3, \cdots z_m$.

Aus diesen Betrachtungen geht hervor, dass die Wurzeln $(z_1, z_2, \cdots z_m)$ einer Gleichung $f(z_1, z_2, \cdots z_m) = 0$ aus der m-fachen, durch die Veränderlichen $z_1, z_2, \cdots z_m$ gegebenen stetigen Mannigfaltigkeit eine $(m-1)$-fach stetige Mannigfaltigkeit herausheben.

§ 354. Aehnliche Ueberlegungen, wie die bisher in dieser Vorlesung durchgeführten, kann man an ein System von Gleichungen mit m Unbekannten $z_1, z_2, \cdots z_m$ zu knüpfen suchen. Hierbei stösst man aber sofort auf eine Reihe von fundamentalen Fragen, deren Erledigung zunächst zu erstreben ist. Während bei einer Gleichung $f(z_1, z_2, \cdots z_m) = 0$ durch Fixirung der Werte von $z_2, \cdots z_m$ die Frage auf eine Gleichung mit einer einzigen Unbekannten gewendet wurde, ist hier über die Existenz von Wurzeln eines Systems von m Gleichungen mit ebenso vielen Unbekannten noch gar nichts bekannt. Es muss also zunächst die Entscheidung über folgende Fragen herbeigeführt werden:

Giebt es Werthsysteme $(z_1, z_2, \cdots z_m)$ der m Variablen z, durch welche m Gleichungen derselben Variablen gleichzeitig erfüllt werden?

Wieviele derartige Wurzeln des Systems giebt es?

Auf welchem Wege können diese Wurzeln gefunden werden, oder wie lässt sich das Problem auf die Lösung einer Gleichung mit einer Unbekannten zurückführen?

Den Weg zur Lösung dieser Probleme liefert die Theorie der Elimination. Durch passende Verbindungen der Gleichungspolynome werden neue Gleichungen hergeleitet, welche weniger als m Unbekannte enthalten. Von den übrigen sagt man, sie seien eliminirt worden. Diese neuen Gleichungen sind Folgen der ursprünglichen; sie werden mit ihnen gleichzeitig befriedigt. Dadurch wird das Problem reducirt, indem man jetzt die neuen Gleichungen an der Stelle der gegebenen behandelt.

Es wird angethan sein, das Problem der Elimination zunächst an zwei Gleichungen mit zwei Unbekannten durchzunehmen.

Dreiunddreissigste Vorlesung.

Elimination bei zwei Gleichungen mit zwei Unbekannten.

§ 355. Es seien zwei Functionen $f_1(z_1, z_2)$ und $f_2(z_1, z_2)$ der Dimensionen m und n vorgelegt. Diese wollen wir uns nach § 340 bereits so zubereitet denken, dass sie die Glieder $c_1 z_1^m$, $c_2 z_2^m$ und $d_1 z_1^n$, $d_2 z_2^n$ enthalten. Wir wollen derartig zubereitete Functionen kurz: präparirte nennen. Ein allgemeines Gleichungssystem ist an sich schon präparirt. Ueber den Einfluss der vorgenommenen Transformation auf das Bestehen von Wurzeln können wir leicht in's Klare kommen, wie im § 356 gezeigt werden wird.

In § 136, Bd. I haben wir die charakteristischen Bedingungen dafür abgeleitet, dass zwei ganze Functionen einer Variablen z

$$(1)\qquad \begin{aligned} f(z) &= a_0 z^m + a_1 z^{m-1} + a_2 z^{m-2} + \cdots + a_m, \\ g(z) &= b_0 z^n + b_1 z^{n-1} + b_2 z^{n-2} + \cdots + b_n \end{aligned}$$

einen gemeinsamen Theiler besitzen. Als Resultat stellte sich heraus, dass eine gewisse ganze Function der Coefficienten a und b, nämlich die Resultante $R_{f,g}$ verschwinden muss. Diese Resultante zeigte sich in den b homogen vom m^{ten}, in den a homogen vom n^{ten} Grade und

in beiden Coefficientenreihen isobarisch vom Gewichte $m \cdot n$, wenn jeder Coefficient als Gewicht den Werth seines Index erhielt.

Nehmen wir nun in (1) statt z die Variable z_1 und setzen für die Coefficienten a und b Functionen einer zweiten Variablen z_2

$$(2)\quad \begin{aligned} a_{m-\lambda} &= a_{\lambda 0} + a_{\lambda 1} z_2 + a_{\lambda 2} z_2^2 + \cdots + a_{\lambda, m-\lambda} z_2^{m-\lambda} \quad (\lambda = 0, 1, \cdots m), \\ b_{n-\lambda} &= b_{\lambda 0} + b_{\lambda 1} z_2 + b_{\lambda 2} z_2^2 + \cdots + b_{\lambda, n-\lambda} z_2^{n-\lambda} \quad (\lambda = 0, 1, \cdots n), \end{aligned}$$

dann können wir die Functionen (1) durch richtige Wahl der $a_{\lambda\mu}$, $b_{\lambda\mu}$ mit den vorgelegten Functionen der beiden Gleichungen

$$(3)\qquad f_1(z_1, z_2) = 0, \quad f_2(z_1, z_2) = 0$$

identificiren; denn die Substitution von (2) in (1) liefert ja die allgemeinste Form für zwei Functionen m^{ter} und n^{ter} Dimension. Tragen wir (2) auch in die Resultante $R_{f,g}$ ein, so entsteht eine Function von z_2, welche wir die Eliminante von f_1 und f_2 in z_2 nennen wollen. Da es sich hier vorläufig nur um zwei Gleichungen (3) handelt, so können wir kürzer

$$(4)\qquad R_{f_1, f_2}(z_2) = R(z_2)$$

schreiben. Die Bezeichnung „Resultante" wollen wir für einen besonderen Fall aufsparen, welcher die bisherige Benennung in sich fasst.

Es bleibt $R(z_2)$ natürlich auch in den $a_{\lambda\mu}$ homogen vom Grade n und in den $b_{\lambda\mu}$ homogen vom Grade m. Hinsichtlich der Gewichte wollen wir folgende Festsetzungen machen: es möge jedem $a_{\lambda\mu}$ das Gewicht $(m-\lambda-\mu)$, jedem $b_{\lambda\mu}$ das Gewicht $(n-\lambda-\mu)$ beigelegt werden. Dadurch ist erreicht, dass, wenn wir z_1 und z_2 je mit dem Gewichte (1) versehen, jedes Glied in

$$(5)\qquad f_1(z_1, z_2) = \sum_{\lambda+\mu=0}^{m} a_{\lambda\mu} z_1^{\lambda} z_2^{\mu}, \quad f_2(z_1, z_2) = \sum_{\lambda+\mu=0}^{n} b_{\lambda\mu} z_1^{\lambda} z_2^{\mu}$$

bezw. das Gewicht m und n besitzt, so dass f_1 isobar mit dem Gewichte m, und f_2 isobar mit dem Gewichte n wird. Man kann dieselbe Bestimmung auch dadurch erreichen, dass man f_1 und f_2 durch Einführung einer neuen Variablen t homogen vom Grade m, bezw. n macht und jedem Coefficienten als Gewicht den Exponenten von t giebt, der seinem Potenzproducte angehört. Dann ist es ersichtlich: $R(z_2)$ ist in den $a_{\lambda\mu}$, $b_{\lambda\mu}$, z_2 isobarisch vom Gewichte mn; $R(z_2)$ steigt also in z_2 höchstens bis zu dem Grade mn auf.

Wenn ζ_2 eine Wurzel der Eliminantengleichung $R(z_2) = 0$ ist, dann haben, wegen der Eigenschaft der Resultanten,

$$(6)\qquad f_1(z_1, \zeta_2), \quad f_2(z_1, \zeta_2)$$

einen gemeinsamen Factor, und also die Gleichungen in z_1

(6ᵃ) $$f_1(z_1, \zeta_2) = 0, \quad f_2(z_1, \zeta_2) = 0$$

gemeinsame Wurzeln. Und umgekehrt, wenn (ζ_1, ζ_2) eine Wurzel von (3) ist, dann haben (6ᵃ) gemeinsame Wurzeln, folglich (6) gemeinsame Factoren, und demnach ist $R(\zeta_2) = 0$. Das zeigt: Um für (3) alle Wurzeln zu finden, bestimmt man (4), sucht alle Wurzeln $\zeta_{2\alpha}$ der Eliminantengleichung in z_2 und bestimmt zu jedem $\zeta_{2\alpha}$ den grössten gemeinsamen Theiler $d_\alpha(z_1, \zeta_{2\alpha})$ von $f_1(z_1, \zeta_{2\alpha})$ und $f_2(z_1, \zeta_{2\alpha})$. Die Wurzeln von $d_\alpha = 0$ mögen $\zeta_{1\alpha}^{(1)}, \zeta_{1\alpha}^{(2)}, \cdots$ sein. Dann haben wir in

$$z_1 = \zeta_{1\alpha}^{(\beta)}, \quad z_2 = \zeta_{2\alpha}$$

sämmtliche Wurzeln von (3).

§ 356. Wir können jetzt an einem einfachen Beispiele die Wirkung der vorläufigen Transformation von § 340 zeigen. Es sei das nicht präparirte System

$$f_1 \equiv z_1 z_2 - 1 = 0, \quad f_2 \equiv z_1 z_2 + z_2^2 - 2 = 0$$

gegeben. Für dieses wird die Eliminantengleichung in z_2

$$R(z_2) = z_2^3 - z_2 = 0,$$

und man erhält die Wurzeln $\zeta_2 = +1;\ -1;\ 0$. Für sie gehen die Gleichungen und die Wurzeln über in

$$\begin{array}{lll} z_1 - 1 = 0, & z_1 - 1 = 0; & (\zeta_{11}, \zeta_{21}) = (1, 1); \\ -z_1 - 1 = 0, & -z_1 - 1 = 0; & (\zeta_{12}, \zeta_{22}) = (-1, -1); \\ 0 \cdot z_1 - 1 = 0, & 0 \cdot z_1 - 2 = 0; & (\zeta_{13}, \zeta_{23}) = (\infty, 0). \end{array}$$

In diesem letzten Falle besteht also kein gemeinsamer Theiler zwischen $f_1(z_1, 0)$, $f_2(z_1, 0)$ im eigentlichen Sinne, und das erklärt sich durch das Auftreten einer Wurzel $z_1 = \infty$ für einen endlichen Werth $z_2 = 0$. In geometrischer Darstellung würde es heissen: die Curven $f_1 = 0$, $f_2 = 0$ haben einen unendlich fernen Punkt in der Richtung einer der Coordinatenaxen gemeinsam. Bei diesen Verhältnissen kann es also geschehen, dass die Eliminanten $R(z_2)$ und $R(z_1)$ in ihren Graden nicht übereinstimmen, auch wenn zu jedem ζ_1 nur ein ζ_2 gehört, welches mit ihm zusammen eine Wurzel bildet. So ist in unserem obigen Beispiele die Eliminante in z_1 nur vom zweiten Grade

$$R(z_1) = -z_1^2 + 1.$$

Um diese Ungleichmässigkeiten zu entfernen, legen wir unseren Betrachtungen präparirte Systeme zu Grunde. Bei diesen ist es nämlich durch das Vorkommen von $c_1 z_1^m$, $c_2 z_2^m$; $d_1 z_1^n$, $d_2 z_2^n$ ausgeschlossen, dass nur eine Coordinate einer Wurzel (ζ_1, ζ_2) des Systems unendlich

gross wird. Ob freilich die beiden Eliminanten von demselben Grade werden, steht auch jetzt noch nicht fest, da möglicherweise zu einem ζ_1 mehrere ζ_2 gehören können, oder umgekehrt.

§ 357. Die Berechnung der zu einem $\zeta_{2\alpha}$ gehörigen Werthe $\zeta_{1\alpha}^{(\beta)}$ wurde in § 355 von der Auflösung der Gleichung $d_\alpha(z_1, \zeta_{2\alpha}) = 0$ abhängig gemacht. Im Allgemeinen wird diese vom ersten Grade sein, doch kann sie auch zu höheren Graden aufsteigen. Durch die im § 149, Bd. I abgeleiteten Resultate werden wir aber der Mühe überhoben, den Teiler d_α aufzusuchen und die Gleichung aufzulösen. Dies wollen wir besprechen, uns dabei aber freilich hier, wie auch dort, auf den Fall beschränken, dass d_α von keinem höheren als dem zweiten Grade ist. Wir können dann aus der dortigen Formel (12) im Falle, dass d_α vom ersten Grade wird, das Resultat ablesen

$$(7)\quad \begin{aligned} 1 : \zeta_{1\alpha} : \zeta_{1\alpha}^2 : \cdots &= \frac{\partial}{\partial a_m} R(\zeta_{2\alpha}) : \frac{\partial}{\partial a_{m-1}} R(\zeta_{2\alpha}) : \frac{\partial}{\partial a_{m-2}} R(\zeta_{2\alpha}) : \cdots \\ &= \frac{\partial}{\partial b_n} R(\zeta_{2\alpha}) : \frac{\partial}{\partial b_{n-1}} R(\zeta_{2\alpha}) : \frac{\partial}{\partial b_{n-2}} R(\zeta_{2\alpha}) : \cdots. \end{aligned}$$

Ist der Theiler d_α von höherem Grade, so sind natürlich auch höhere Gleichungen aufzulösen. Die dortige Formel (16) giebt für den Fall eines quadratischen d_α die beiden Wurzeln $\zeta_{1\alpha}^{(1)}$, $\zeta_{1\alpha}^{(2)}$ als Wurzeln von

$$(8)\quad \frac{\partial^2}{\partial a_{k+1}^2} R(\zeta_{2\alpha}) z_1^2 - 2\frac{\partial^2}{\partial a_{k+1}\,\partial a_k} R(\zeta_{2\alpha}) z_1 + \frac{\partial^2}{\partial a_k^2} R(\zeta_{2\alpha}) = 0 .$$

§ 358. Die Frage, auf welche Weise die etwa vorhandenen Wurzeln zweier Gleichungen mit zwei Unbekannten zu bestimmen seien, ist durch die bisherigen Untersuchungen zwar erledigt, aber ohne dass dabei Resultate über die Anzahl der Wurzeln zu Tage getreten wären. Damit wollen wir uns jetzt beschäftigen.

Es kann vorkommen (§ 348, XI), dass überhaupt keine Wurzeln für die beiden Gleichungen (3) bestehen, wie dies ja auch schon das einfache Beispiel

$$z_1^2 - z_2^2 + 1 = 0, \quad z_1 - z_2 = 0$$

zeigt. Es kann ferner vorkommen, dass die beiden Gleichungen unendlich viele Wurzeln besitzen, wie dies in dem Falle eintritt, dass f_1 und f_2 einen gemeinsamen Theiler aufweisen. Welches ist der, sozusagen, allgemeine Fall, und wie gehen aus ihm die möglichen Besonderheiten hervor?

Bei der Bildung der Eliminante $R(z_2)$ wollen wir in allen einzelnen Elementen der Determinante $(m+n)^{\text{ter}}$ Ordnung stets nur das Glied beibehalten, welches die höchste Potenz in z_2 enthält. Dadurch entsteht unter Benutzung der Bezeichnungen (2) und (5)

$$\begin{vmatrix} a_{m0}, & a_{m-1,1}\cdot z_2, & a_{m-2,2}\cdot z_2^2, & \cdots & a_{0,m}\cdot z_2^m, & 0, & \cdots \\ 0, & a_{m,0}, & a_{m-1,1}\cdot z_2, & \cdots & a_{1,m-1}\cdot z_2^{m-1}, & a_{0m}\, z_2^m, & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{n0}, & b_{n-1,1}\cdot z_2, & b_{n-2,2}\cdot z_2^2, & \cdots & b_{0,n}\cdot z_2^n, & 0, & \cdots \\ 0, & b_{n0}, & b_{n-1,1}\cdot z_2, & \cdots & b_{1,n-1}\cdot z_2^{n-1}, & b_{0n}\, z_2^n, & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Multiplicirt man nun die zweite, dritte, $\cdots n^{te}$ Zeile mit $z_2, z_2^2, \cdots z_2^{n-1}$, dann die $(n+2)^{te}$, $(n+3)^{te}$, $\cdots (n+m)^{te}$ Zeile mit $z_2, z_2^2, \cdots z_2^{m-1}$, so kann man aus jeder k^{ten} Spalte z_2^{k-1} herausziehen. Dadurch erhält man für die Determinante den Werth

$$(9) \qquad \begin{vmatrix} a_{m0}, & a_{m-1,1}, & a_{m-2,2}, & \cdots & a_{0m}, & 0, & 0, \cdots \\ 0, & a_{m0}, & a_{m-1,1}, & \cdots & a_{1,m-1}, & 0_{0m}, & 0, \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{n0}, & b_{n-1,1}, & b_{n-2,2}, & \cdots & b_{0,n}, & 0, & 0, \cdots \\ 0, & b_{n0}, & b_{n-1,1}, & \cdots & b_{1,n-1}, & b_{0n}, & 0, \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} \cdot z_2^{mn}.$$

Hier ist der Factor von z_2^{mn} gleich der Resultante zweier Functionen

$$(10) \qquad \begin{aligned} \chi_1(t) &= a_{m0} + a_{m-1,1}\, t + a_{m-2,2}\, t^2 + \cdots + a_{0m}\, t^m, \\ \chi_2(t) &= b_{n0} + b_{n-1,1}\, t + b_{n-2,2}\, t^2 + \cdots + b_{0n}\, t^n. \end{aligned}$$

Die Bedeutung dieses Resultates ergiebt sich, wenn man die Functionen f_1 und f_2 nach den fallenden Dimensionen ihrer Glieder ordnet,

$$(11) \qquad \begin{aligned} f_1 &= u_m(z_1, z_2) + u_{m-1}(z_1, z_2) + \cdots + u_1(z_1, z_2) + u_0, \\ f_2 &= v_n(z_1, z_2) + v_{n-1}(z_1, z_2) + \cdots + v_1(z_1, z_2) + v_0; \end{aligned}$$

$$(12) \qquad \begin{aligned} u_\lambda(z_1, z_2) &= a_{\lambda,0}\, z_1^\lambda + a_{\lambda-1,1}\, z_1^{\lambda-1} z_2 + \cdots + a_{0,\lambda}\, z_2^\lambda, \\ v_\lambda(z_1, z_2) &= b_{\lambda,0}\, z_1^\lambda + b_{\lambda-1,1}\, z_1^{\lambda-1} z_2 + \cdots + b_{0,\lambda}\, z_2^\lambda, \end{aligned}$$

wobei also z. B. u_λ alle Glieder λ^{ter} Dimension in z_1 und z_2 umschliesst, welche f_1 enthält. Hieraus entnehmen wir

$$\chi_1(t) = u_m(1, t), \qquad \chi_2(t) = v_n(1, t),$$

so dass, wenn $\chi_1(t)$ und $\chi_2(t)$ keinen gemeinsamen Theiler haben, dies auch bei $u_m(1, t)$, $v_n(1, t)$ und also auch bei $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ nicht vorkommt, und umgekehrt. In diesem und nur in diesem Falle, dass kein solcher Theiler besteht, ist (9) von 0 verschieden, und $R(z_2)$ erhebt sich bis zum Grade $m \cdot n$.

Die beiden Functionen $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ sind homogen, so dass $u_m = 0$, $v_n = 0$ die banale Wurzel $(0, 0)$ besitzen. Ausser ihr kommt nur dann eine Wurzel vor, wenn $R_{\chi_1, \chi_2} = 0$ ist. Diese Resul-

tante wollen wir auch mit R_{u_m, v_n} bezeichnen und die Resultante der beiden homogenen Functionen u_m und v_n nennen.

Wir haben dann das Resultat: Wenn die Resultante $R_{u_m, v_n} \neq 0$ ist, d. h. wenn kein (z_1, z_2) ausser $(0, 0)$ besteht, welches die Glieder höchster Dimension in f_1 und in f_2 zum Verschwinden bringt, dann und nur dann steigt die Eliminante $R(z_2)$ zum Grade $m \cdot n$ auf.

Dieser Fall kann als der allgemeine bezeichnet werden, da die beiden ganzen Functionen (10) im Allgemeinen keine gemeinsame Wurzel besitzen. Man kann ja, selbst bei festem $\chi_1(t)$, das $\chi_2(t)$ immer noch auf unendlich viele Arten so bestimmen, dass $R_{\chi_1, \chi_2} \neq 0$ wird.

§ 359. Unsere Betrachtungen zeigen ebenso, dass $R(z_1)$ im Allgemeinen bis zum Grade $m \cdot n$ aufsteigt. Aber gleichwohl ist daraus direct noch kein Schluss auf die Anzahl der Wurzeln möglich. Denn es ist ja bei den präparirten Gleichungen freilich ausgeschlossen, dass zu einem $z_2 = \zeta_2$ ein unendliches, und also nicht aus $R(z_1) = 0$ zu entnehmendes z_1 eingeht; aber es wäre möglich, dass zu einem ζ_2' mehrere $\zeta_1', \zeta_1'', \zeta_1''', \cdots$ und zu ζ_2'' gleichfalls $\zeta_1'', \zeta_1^{(IV)}, \cdots$ gehörten. Dabei wäre die Anzahl der Wurzeln nicht zu überblicken.

Dass aber die wirkliche Anzahl der endlichen Wurzeln bei präparirten Gleichungen mit der Gradzahl der Eliminante $R(z_2)$ übereinstimmt, und zwar auch dann, wenn durch irgend welche Besonderheiten der Functionen f_1 und f_2 dieser Grad geringer als $m \cdot n$ sein sollte, das lässt sich auf dem folgenden, von Liouville*) hierzu benutztem Wege nachweisen.

Wir führen in f_1 und in f_2 statt z_2 eine neue Variable x durch die Substitutionen

$$(13) \qquad x = \varkappa z_1 + \lambda z_2, \quad z_2 = \frac{x - \varkappa z_1}{\lambda}$$

ein, wobei $\varkappa, \lambda$ unbestimmte gewichtlose Parameter bedeuten, so dass also die neue Variable x auch vom Gewichte 1 wird, wie z_1 und z_2. Da $\varkappa, \lambda$ unbestimmt sind, so entspricht jeder Wurzel (ζ_1, ζ_2) auch ein $x = \xi$ und umgekehrt jedem $x = \xi$ ein (ζ_1, ζ_2). Zwei Wurzelpunkten (ζ_1', ζ_2') und (ζ_1'', ζ_2''), die nicht in beiden Coordinatenpaaren übereinstimmen, entsprechen verschiedene ξ', ξ''. Wir tragen nun (13) in (3) ein; dann erhält f_1 als höchsten Nenner λ^m, und f_2 als höchsten Nenner λ^n. Setzen wir demnach

$$(14) \quad \lambda^m f_1\left(z_1, \frac{x - \varkappa z_1}{\lambda}\right) = g_1(z_1, x), \qquad \lambda^n f_2\left(z_1, \frac{x - \varkappa z_1}{\lambda}\right) = g_2(z_1, x),$$

dann sind g_1 und g_2 ganze Functionen in $z_1, x, \varkappa, \lambda$.

*) J. d. Math. p. e. a. (1); 12 (1847), p. 68—72.

Nun bilden wir die Eliminantengleichung

(15) $$R_{g_1, g_2}(x) = 0$$

und betrachten eine ihrer Wurzeln ξ. Die beiden Functionen $g_1(z_1, \xi)$ und $g_2(z_1, \xi)$ besitzen dann einen gemeinsamen Factor, und daher

$$f_1\left(z_1, \frac{\xi - \varkappa z_1}{\lambda}\right) = 0, \quad f_2\left(z_1, \frac{\xi - \varkappa z_1}{\lambda}\right) = 0$$

eine gemeinsame Wurzel $z_1 = \zeta_1$. Folglich haben $f_1(z_1, z_2) = 0$, $f_2(z_1, z_2) = 0$ die Wurzel

$$z_1 = \zeta_1, \quad z_2 = \frac{\xi - \zeta_1 \varkappa}{\lambda}.$$

Diese Wurzel ist natürlich von $\varkappa, \lambda$ unabhängig, weil f_1 und f_2 es sind. Daher muss ζ_1 von $\varkappa$ und λ unabhängig sein. Ferner muss $(\xi - \zeta_1\varkappa)$ von $\varkappa$ unabhängig und durch λ theilbar sein; setzen wir also $(\xi - \zeta_1\varkappa) = \zeta_2\lambda$, so folgt, dass auch ζ_2 von $\varkappa$ und λ unabhängig ist. Wir haben also $z_2 = \zeta_2$ und $\xi = \varkappa\zeta_1 + \lambda\zeta_2$. Alle Wurzeln von (15) haben die Form

$$x = \xi_\alpha = \varkappa\zeta_{1\alpha} + \lambda\zeta_{2\alpha},$$

wobei $\zeta_{1\alpha}$, $\zeta_{2\alpha}$ von $\varkappa$ und λ unabhängig bleiben. Hat man sämmtliche Wurzeln von (15) in der Gestalt

$$\xi_\alpha(\varkappa, \lambda) = \varkappa\zeta_{1\alpha} + \lambda\zeta_{2\alpha} \qquad (\alpha = 1, 2, \cdots)$$

bestimmt, so erhält man sämmtliche Wurzeln von

(3) $$f_1(z_1, z_2) = 0, \quad f_2(z_1, z_2) = 0$$

in der Gestalt

$$(\xi_1(1,0),\ \xi_1(0,1)), \quad (\xi_2(1,0),\ \xi_2(0,1)), \cdots.$$

Besitzt (15) den Factor $(x - \xi)$ genau in der q^{ten} Potenz, dann wollen wir das entsprechende (ζ_1, ζ_2) eine q-fache Wurzel des Systems (3) nennen. Bei dieser Festsetzung giebt der Grad von $R_{g_1, g_2}(x)$ die Anzahl der endlichen Wurzeln des Systems (3) an.

§ 360. Wir setzen die Eliminante

(16) $$R_{g_1, g_2}(x) = \varrho_0(\varkappa, \lambda) \cdot x^k - \varrho_1(\varkappa, \lambda) \cdot x^{k-1} + \varrho_2(\varkappa, \lambda) \cdot x^{k-2} - \cdots.$$

Im allgemeinen Falle ist $k = m \cdot n$. Die Wurzeln von $R(x) = 0$ sind von der Form $\varkappa\zeta_1 + \lambda\zeta_2$, wo ζ_1 und ζ_2 endliche Grössen bedeuten. Es kann also für kein endliches Werthepaar $\varkappa, \lambda$ eine Wurzel x unendlich gross werden. Dies müsste nun aber geschehen, wenn irgend eine Wurzel $(\varkappa_0, \lambda_0)$ von $\varrho_0(\varkappa, \lambda) = 0$ nicht zugleich Wurzel aller $\varrho_1(\varkappa, \lambda) = 0$, $\varrho_2(\varkappa, \lambda) = 0, \cdots$ wäre. Die Coefficienten $\varrho_1, \varrho_2, \cdots$ verschwinden sonach für alle Werthsysteme, welche $\varrho_0 = 0$ machen.

Nach § 348, (X) kann man daher alle irreductiblen Factoren von ϱ_0 aus $\varrho_1, \varrho_2, \cdots$ herausheben. Ist dies geschehen, und bleiben dann noch weitere Factoren von ϱ_0 zurück, dann gelten dieselben Schlüsse. Wir können deshalb alle Theiler von ϱ_0, welche überhaupt von $\varkappa, \lambda$ abhängen, aus allen ϱ herausheben. Setzen wir daher $R(x) = 0$, so dürfen wir von vornherein die höchste Potenz von x mit einem von $\varkappa$ und λ freien Coefficienten versehen. Diesen können wir jetzt im Falle unbestimmter Coefficienten $a_{\lambda\mu}$, $b_{\lambda\mu}$ leicht berechnen. Setzen wir $\varkappa = 0$, $\lambda = 1$, dann geht x in z_2 und $R_{g_1, g_2}(x)$ in $R_{f_1, f_2}(z_2)$ über. Nach § 358 ist in der letzten Function der höchste Coefficient R_{v_m, v_n}; und deswegen haben wir auch hier

$$(17) \qquad \varrho_0(\varkappa, \lambda) = R_{v_m, v_n}.$$

Da die Wurzeln von (15) die Form $(\varkappa\zeta_1 + \lambda\zeta_2)$ haben, und da ferner

$$\frac{\varrho_1(\varkappa, \lambda)}{\varrho_0(\varkappa, \lambda)} = + S(\varkappa\zeta_{1\alpha} + \lambda\zeta_{2\alpha}),$$

$$\frac{\varrho_2(\varkappa, \lambda)}{\varrho_0(\varkappa, \lambda)} = + S(\varkappa\zeta_{1\alpha} + \lambda\zeta_{2\alpha})(\varkappa\zeta_{1\beta} + \lambda\zeta_{2\beta}), \cdots$$

ist, so folgt, dass ϱ_1 homogen und linear in $\varkappa, \lambda$ ist, ϱ_2 homogen und quadratisch in $\varkappa, \lambda$, u. s. w., unter der Voraussetzung, dass ϱ_0 bereits von $\varkappa$ und λ frei gemacht worden ist.

Der erste Coefficient ϱ_0 hat in den $a_{\lambda\mu}$, $b_{\lambda\mu}$ das Gewicht 0, denn nach § 358 gehen in ihn nur $a_{m0}, a_{m-1,1}, \cdots; b_{n0}, b_{n-1,1}, \cdots$ ein, und alle diese Coefficienten haben gemäss § 355 das Gewicht 0.

Weiter folgt dann aus den letzten Formeln, da $\zeta_{1\alpha}$ und $\zeta_{2\alpha}$ das Gewicht 1 besitzen, dass ϱ_1 isobarisch vom Gewichte 1, ϱ_2 vom Gewichte 2 ist u. s. f.; alles bezüglich der Coefficientenreihen $a_{\lambda\mu}$ und $b_{\lambda\mu}$.

Die Substitution (13) wandelt f_1, f_2 in homogene lineare Functionen der $a_{\lambda\mu}$ bez. der $b_{\lambda\mu}$ um. Leitet man nun (16) mit Hülfe der Determinantenform her (§ 151, Bd. I), dann folgt, dass (16) und also auch jedes einzelne $\varrho_\varkappa$ in den $a_{\lambda\mu}$ homogen vom Grade n und in den $b_{\lambda\mu}$ vom Grade m ist.

Wir sammeln die erhaltenen Resultate in folgenden Sätzen: Führt man bei allgemeinen Functionen f_1, f_2 die Substitution (13) durch und erhält dabei g_1, g_2, so ist

$$(16) \quad R_{g_1, g_2}(x) = \varrho_0(\varkappa, \lambda)x^k - \varrho_1(\varkappa, \lambda)x^{k-1} + \varrho_2(\varkappa, \lambda)x^{k-2} - \cdots$$

vom Grade $k = m \cdot n$. Sämmtliche ϱ sind homogen in den $a_{\lambda\mu}$ vom Grade n und in den $b_{\lambda\mu}$ vom Grade m; ferner hat ϱ_α in den beiden Coefficientenreihen das Gewicht α. Es ist ϱ_0 von $\varkappa$ und λ unabhängig und

(17) $$\varrho_0 = R_{u_m, v_n};$$

nach § 153, Bd. I ist dies eine irreductible Function. ϱ_α ist in den $\varkappa, \lambda$ homogen vom Grade α.

Wenn für besondere Werte der $a_{\lambda\mu}$, $b_{\lambda\mu}$ die Grössen ϱ_0, $\varrho_1, \cdots \varrho_{\mu-1}$ identisch d. h. für alle Werte von $\varkappa$ und λ verschwinden, dann ist der von $\varkappa$ und λ unabhängige Theiler von ϱ_μ in allen folgenden $\varrho_{\mu+1}$, $\varrho_{\mu+2}, \cdots$ enthalten und kann aus der Eliminantengleichung herausgehoben werden.

Aus (16) folgt, wenn man

$$\varrho_\alpha(\varkappa, \lambda) = \varrho_\alpha' \varkappa^\alpha + \varrho_\alpha'' \varkappa^{\alpha-1}\lambda + \varrho_\alpha''' \varkappa^{\alpha-2}\lambda^2 + \cdots$$

setzt, eine Reihe von Formeln der Gestalt

$$\varrho_0 S(\zeta_{1\varkappa}) = \varrho_1(1, 0), \quad \varrho_0 S(\zeta_{2\varkappa}) = \varrho_1(0, 1);$$

$$\varrho_0 S(\zeta_{1\varkappa}\zeta_{1\lambda}) = \varrho_2', \quad \varrho_0 S(\zeta_{1\varkappa}\zeta_{2\lambda}) = \varrho_2'', \quad \varrho_0 S(\zeta_{2\varkappa}\zeta_{2\lambda}) = \varrho_2''';$$

. . . .

§ 361. Wir können jetzt leicht die Frage entscheiden, in welcher Beziehung die Grade von $R_{f_1, f_2}(z_2)$, $R_{f_1, f_2}(z_1)$ und $R_{g_1, g_2}(x)$ zueinander stehen. Es ist bereits erwähnt worden, dass durch die Annahme $\varkappa = 0$, $\lambda = 1$ das $R(x)$ in $R(z_2)$ übergeht, ohne dass der erste Coefficient verschwinde. Beide Eliminanten stimmen demnach im Grade überein, und das Gleiche gilt offenbar von $R(z_1)$, wie die Annahme $\varkappa = 1$, $\lambda = 0$ zeigt. Denn setzen wir

$$\varkappa^m f_1\left(\frac{x - \lambda z_2}{\varkappa}, z_2\right), \quad \varkappa^n f_2\left(\frac{x - \lambda z_2}{\varkappa}, z_2\right)$$

als neue Functionen an und suchen von ihnen die Eliminante in x, so wird sie ihrer Bedeutung nach mit (16) bis auf einen constanten Factor übereinstimmen, da beide $\xi_1, \xi_2, \cdots$ zu Wurzeln haben.

Es muss aber auch hier hervorgehoben werden, dass diese Resultate nur für präparirte Gleichungssysteme richtig sind. Anderenfalls können $R(z_1)$, $R(z_2)$ einzeln oder beide von höherem Grade werden als $R(x)$. So hat man z. B. für

$$f_1(z_1, z_2) = z_1 z_2 - 1, \quad f_2(z_1, z_2) = z_1 z_2^2 + z_1 - 2$$

die drei Eliminanten

$$R_{f_1, f_2}(z_1) = 2z_1(z_1 - 1), \quad R_{f_1, f_2}(z_2) = -2z_2(z_2 - 1),$$
$$R_{g_1, g_2}(x) = 4\varkappa^2\lambda^2(x - \varkappa - \lambda).$$

Aus der letzten Form ergiebt sich die einzige endliche Wurzel von $f_1 = 0$, $g_1 = 0$, nämlich $\zeta_1 = \zeta_2 = 1$. Die Substitution von $z_1 = 0$ und von $z_2 = 0$ in f_1 und in f_2 ruft

$$f_1(0, z_2) = -1, \quad f_2(0, z_2) = -2;$$
$$f_1(z_1, 0) = -1, \quad f_2(z_1, 0) = z_1 - 2$$

hervor. Präparirt man dagegen zuerst f_1, f_2 durch die Substitution

$$z_1 = u_1 + u_2, \quad z_2 = u_1 - u_2,$$

so erhält man

$$\varphi_1(u_1, u_2) = u_1^2 - u_2^2 - 1, \; \varphi_2(u_1, u_2) = u_1^3 + u_1^2 u_2 - u_1 u_2^2 - u_2^3 + u_1 + u_2 - 2$$

und die Eliminanten

$$R_{\varphi_1, \varphi_2}(u_1) = -8(u_1 - 1), \quad R_{\varphi_1, \varphi_2}(u_2) = -8 u_2$$

geben jetzt die richtige Gradzahl 1 an.

Vierunddreissigste Vorlesung.

Uebergang vom allgemeinen zu besonderen Fällen.

§ 362. Wir haben gesehen, dass die Anzahl der Wurzeln des Systems

$$(1) \qquad f_1(z_1, z_2) = \sum_{\lambda+\mu=0}^{m} a_{\lambda\mu} z_1^{\lambda} z_2^{\mu}, \quad f_2(z_1, z_2) = \sum_{\lambda+\mu=0}^{n} b_{\lambda\mu} z_1^{\lambda} z_2^{\mu}$$

im Allgemeinen $m \cdot n$ beträgt, nämlich dann, wenn die $a_{\lambda\mu}$, $b_{\lambda\mu}$ unbestimmte Grössen bedeuten, und wir haben auch erkannt, dass bei speciellen Werthen von $a_{\lambda\mu}$, $b_{\lambda\mu}$ diese Zahl erhalten bleibt, so lange die Glieder höchster Dimensionen in den Functionen, also die der m^{ten} in f_1 und die der n^{ten} in f_2, keinen gemeinsamen Wurzelpunkt besitzen. Wir bezeichnen wie früher die Polynome nach den Dimensionen geordnet

$$(2) \qquad f_1(z_1, z_2) = \sum_{\varkappa=0}^{m} u_\varkappa(z_1, z_2), \quad f_2(z_1, z_2) = \sum_{\varkappa=0}^{n} v_\varkappa(z_1, z_2).$$

Dann kann also eine Gradreduction nur dadurch entstehen, dass die Resultante $R_{u_m, v_n} = 0$ wird.

Wählen wir ein solches Functionenpaar f_1, f_2 zum Ausgangspunkte, bei welchem diese Resultante von Null verschieden, bei dem somit die Anzahl der Wurzeln $m \cdot n$ ist, und wandeln wir die Coefficienten von da aus in stetiger Aenderung so um, dass sie zu denen eines anderen Paares werden, dessen Eliminante nach z_2 nicht bis zum Grade $m \cdot n$ in die Höhe geht, so ist nach § 351 die Gradreduction durch das Unendlichwerden von entsprechend vielen Wurzelcoordinaten z_2 und bei präparirten Gleichungen von entsprechend vielen Wurzeln (z_1, z_2) zu erklären.

Bei geometrischer Repräsentation der Gleichungen durch Curven stellen sich die Verhältnisse recht übersichtlich dar. Haben $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ einen gemeinsamen Factor $(z_1 - \alpha z_2)$, und setzt man

$$z_1 = \varrho \cos \varphi, \quad z_2 = \varrho \sin \varphi,$$

dann werden durch Einführung dieser Polarcoordinaten ϱ und φ

$$f_1(z_1, z_2) = \varrho^m \left[u_m(\cos \varphi, \sin \varphi) + u_{m-1}(\cos \varphi, \sin \varphi)\frac{1}{\varrho} + \cdots\right],$$

$$f_2(z_1, z_2) = \varrho^n \left[v_n(\cos \varphi, \sin \varphi) + v_{n-1}(\cos \varphi, \sin \varphi)\frac{1}{\varrho} + \cdots\right];$$

für sehr grosse ϱ kann man sich auf die Betrachtung der Glieder höchster Dimension, d. h. auf

$$f_1(z_1, z_2) = \varrho^m \cdot u_m(\cos \varphi, \sin \varphi), \qquad f_2(z_1, z_2) = \varrho^n \cdot v_n(\cos \varphi, \sin \varphi)$$

beschränken. Es liefert daher die Bestimmung $\operatorname{cotg} \varphi = z_1 : z_2 = \alpha$ eine Richtung φ, für welche die Curven $f_1 = 0$ und $f_2 = 0$ einen und denselben unendlich fernen Punkt besitzen. Die Existenz eines solchen ist charakteristisch für die Reduction des Grades von $R_{f_1, f_2}(z_2)$.

§ 363. Wir wollen jetzt untersuchen, welche Gradreduction eintritt, wenn $u_m = 0$, $v_n = 0$ eine gemeinsame $\varkappa$-fache Wurzel besitzen, also u_m und v_n einen Factor $(z_1 - \alpha z_2)^\varkappa$. Wir können dabei $\alpha = 0$ setzen, weil dies ja nur auf eine lineare Transformation hinausläuft. Dann wird etwa

$$u_m(z_1, z_2) = a_{m,0}\, z_1^m + a_{m-1,1}\, z_1^{m-1} z_2 + \cdots + a_{\varkappa, m-\varkappa}\, z_1^\varkappa z_2^{m-\varkappa},$$

$$v_n(z_1, z_2) = b_{n,0}\, z_1^n + b_{n-1,1}\, z_1^{n-1} z_2 + \cdots + b_{\lambda, n-\lambda}\, z_1^\lambda z_2^{n-\lambda},$$

wobei $\lambda \geqq \varkappa$ anzusetzen ist. Unter dieser Annahme bilden wir die Eliminante $R(z_2)$ und behalten genau wie in § 358 von jedem ihrer, als ganze Functionen von z_2 auftretenden Elementen die Glieder höchster Dimension zurück. Dann ist die Determinante von der Form:

$$\begin{vmatrix} a_{m,0}, & a_{m-1,1} \cdot z_2, & \cdots & a_{\varkappa,m-\varkappa} \cdot z_2^{m-\varkappa}, & a_{\varkappa-1,m-\varkappa} z_2^{m-\varkappa}, & \cdots & a_{0,m-1} z_2^{m-1}, & 0 \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{n,0}, & b_{n-1,1} \cdot z_2, & \cdots & b_{\lambda,n-\lambda} \cdot z_2^{n-\lambda}, & b_{\lambda-1,n-\lambda} z_2^{n-\lambda}, & \cdots & b_{0,n-1} z_2^{n-1}, & 0 \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Wir gestalten sie so um, dass die zweite und die $(n+2)^{\text{te}}$ Zeile mit z_2, ferner die dritte und die $(n+3)^{\text{te}}$ mit z_2^2, u. s. w. multiplicirt wird; aus der zweiten Spalte ziehen wir dann z_2, aus der dritten $z_2^2, \cdots$ heraus. So entsteht

$$z^{mn} \cdot \begin{vmatrix} a_{m,0}, & a_{m-1,1}, & \cdots & a_{\varkappa,m-\varkappa}, & a_{\varkappa-1,m-\varkappa} z_2^{-1}, & \cdots & a_{0,m-1} z_2^{-1}, & 0 \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{n,0}, & b_{n-1,1}, & \cdots & b_{\lambda,n-\lambda}, & b_{\lambda-1,n-\lambda} z_2^{-1}, & \cdots & b_{0,n-1} z_2^{-1}, & 0 \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Es handelt sich nun darum, die niedrigste Potenz von z_2^{-1} zu bestimmen, die bei der Entwickelung der Determinante auftritt. Offenbar sind die Elemente der $\varkappa$ letzten Spalten durch z_2^{-1} theilbar. Es tritt also jedenfalls $z_2^{-\varkappa}$ heraus, und man erkennt ohne Schwierigkeit, dass eines der dazu gehörigen Glieder, welches bei unbestimmten $a_{\lambda\mu}$, $b_{\lambda\mu}$ durch kein anderes zerstört werden kann, gleich

$$a_{\varkappa, m-\varkappa}^{n}\, b_{0,n}^{\varkappa}\, b_{n,0}^{m-\varkappa}\, z_2^{-\varkappa}$$

ist. Folglich erscheint in $R(z_2)$ die Potenz $z_2^{mn-\varkappa}$ als die höchste, d. h. haben $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ einen Factor $(z_1 - \alpha z_2)^{\varkappa}$ gemeinsam, dann steigt $R(z_2)$ nur bis zum Grade $(m \cdot n - \varkappa)$ auf. Wir können dies geometrisch wieder so ausdrücken, dass wir sagen: die Curven $f_1 = 0$, $f_2 = 0$ haben in der Richtung $\operatorname{cotg} \varphi = \alpha$ unendlich ferne $\varkappa$ Punkte gemeinsam.

§ 364. Wir gehen zu dem besonderen Falle $\varkappa = 1$, $\lambda = 1$ über. Zieht man dabei aus der obigen Determinante den Factor z^{-1} der letzten Spalte heraus, dann findet man den zugehörigen Coefficienten, wenn man in der zurückbleibenden Determinante alle Glieder mit z^{-1} unterdrückt. Hierdurch zerfällt sie aber sofort in ein Product einer Determinante zweiten und einer solchen $(m + n - 2)^{\text{ten}}$ Grades, deren Form als Coefficienten den Werth

$$R_{\varphi_1, \varphi_2} \cdot R_{\psi_1, \psi_2} \tag{3}$$

ergiebt, wenn man setzt

$$\varphi_1 = a_{m,0} + a_{m-1,1}\, t + \cdots + a_{1,m-1}\, t^{m-1} = u_m(1, t),$$
$$\varphi_2 = b_{n,0} + b_{n-1,1}\, t + \cdots + b_{1,n-1}\, t^{n-1} = v_n(1, t),$$
$$\psi_1 = a_{1,m-1} + a_{0,m-1}\, t, \qquad \psi_2 = b_{1,n-1} + b_{0,n-1}\, t.$$

Auch hier wird im Allgemeinen (3) nicht verschwinden, und auch numerische Bestimmungen lassen sich in beliebiger Menge angeben, bei denen dies nicht eintritt. Eine weitere Reduction des Grades der Eliminante $R(z_2)$ kann gemäss (3) auf zwei Arten zu Stande kommen. Die erste Möglichkeit wird durch $R_{\varphi_1, \varphi_2} = 0$ gegeben; das bedeutet, es haben $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ ausser dem einen gemeinsamen Theiler z_1 noch einen anderen Theiler $(z_1 - \beta z_2)$ gemeinsam. Die zweite Möglichkeit wird durch $R_{\psi_1, \psi_2} = 0$ geliefert, d. h. durch das Bestehen der Proportion $a_{1,m-1} : b_{1,n-1} = a_{0,m-1} : b_{0,n-1}$ oder, was dasselbe aussagt, durch das Bestehen der Gleichung

$$\left|\frac{u_m(z_1, z_2)}{v_n(z_1, z_2)}\right|_{z_1=0} = \left|\frac{u_{m-1}(z_1, z_2)}{v_{n-1}(z_1, z_2)}\right|_{z_1=0}.$$

Nun verschwinden für $z_1 = 0$ Zähler und Nenner der linken Seite; deswegen können wir die Relation auch in der Form

$$\left|\frac{\frac{\partial u_m(z_1, z_2)}{\partial z_1}}{u_{m-1}(z_1, z_2)}\right|_{z_1=0} = \left|\frac{\frac{\partial v_n(z_1, z_2)}{\partial z_1}}{v_{n-1}(z_1, z_2)}\right|_{z_1=0}$$

schreiben. Dies drückt, geometrisch gesprochen, nur aus, dass die zu dem gemeinsamen unendlich fern gelegenen Punkte gehörigen Asymptoten beider Curven zusammenfallen.

§ 365. Das Schlussresultat von § 363 lässt sich auch so ausdrücken, dass wir sagen: Haben $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ einen Factor $(z_1 - \alpha z_2)^\varkappa$ gemeinsam, dann besitzen $f_1 = 0$ und $f_2 = 0$ in der Richtung $\operatorname{cotg} \varphi = \alpha$ im Unendlichen $\varkappa$ gemeinsame Punkte. Gesetzt nun, $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ hätten noch einen anderen Factor $(z_1 - \beta z_2)^\lambda$ gemeinsam, dann haben $f_1 = 0$, $f_2 = 0$ auch in der Richtung $\operatorname{cotg} \varphi = \beta$ unendlich fern λ gemeinsame Punkte. Wir machen nun von der Thatsache Gebrauch, dass der Grad der Eliminante um ebensoviele Einheiten vermindert wird, als es unendlich ferne Wurzeln giebt; dies ist dadurch sicher gestellt, dass man von dem allgemeinen Falle den Uebergang zu dem besonderen Systeme vornimmt, oder auch dadurch, dass man $z_1 = \varrho \cos \varphi$, $z_2 = \varrho \sin \varphi$ einführt und die Werthe von $\frac{1}{\varrho}$ betrachtet. Durch diese Thatsache gelangen wir dann zu dem Ergebnisse: Haben $u_m(z_1, z_2)$ und $v_n(z_1, z_2)$ einen Factor der Dimension μ gemeinsam, dann steigt die Eliminante $R(z_2)$ von $f_1 = 0$ und $f_2 = 0$ in z_2 höchstens bis zum Grade $(mn - \mu)$ auf.

Wir haben diesen Satz nicht auf rein arithmetischem Wege hergeleitet. Ein Beweis desselben, der sich ausschliesslich auf determinanten-theoretische Betrachtungen stützt, wäre sehr erwünscht; er scheint aber nicht gerade einfach zu sein.

§ 366. Wir wenden uns nun zu dem Falle, dass $f_1 = 0$ eine Wurzel (ζ_1, ζ_2) in der k-fachen, und $f_2 = 0$ dieselbe Wurzel in der l-fachen Multiplicität besitzt, und fragen, in welcher Multiplicität (ζ_1, ζ_2) als Wurzel des Systems $f_1 = 0$, $f_2 = 0$ aufzufassen ist.

Bevor wir dieser Frage näher treten, wollen wir, um eine spätere Unterbrechung zu vermeiden, einen für uns nothwendigen Satz aus der Theorie der Resultanten herleiten*).

Wir setzen, indem wir unter ϱ einen willkürlichen Parameter verstehen,

$$(4)\quad \begin{aligned} f_1(z) &= a_0\varrho^k + a_1\varrho^{k-1}z + \cdots + a_{k-1}\varrho z^{k-1} + a_k z^k + a_{k+1}z^{k+1} + \cdots + a_m z^m, \\ g_1(z) &= b_0\varrho^l + b_1\varrho^{l-1}z + \cdots + b_{l-1}\varrho z^{l-1} + b_l z^l + b_{l+1}z^{l+1} + \cdots + b_n z^n, \end{aligned}$$

*) Fr. Meyer, Ueber die Structur der Discriminanten und Resultanten binärer Formen. Gött. N. 1895 Heft 1; vgl. auch ibid. Heft 2.

wobei k und l zwei positive, ganze Zahlen sind, von denen k nicht kleiner als l sein soll. Wir schreiben die Resultante R von f_1 und g_1 nach z in der gewöhnlichen Form als Determinante $(m+n)^{\text{ter}}$ Ordnung, indem wir unter die ersten l Zeilen mit den Coefficienten a die ersten k Zeilen mit den Coefficienten b hinschreiben, nämlich

$$\left.\begin{matrix} a_0\varrho^k & a_1\varrho^{k-1} & a_2\varrho^{k-2} \cdots \\ 0 & a_0\varrho^k & a_1\varrho^{k-1} \cdots \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot\;\cdot \end{matrix}\right\} l \text{ Zeilen}$$

$$\left.\begin{matrix} b_0\varrho^l & b_1\varrho^{l-1} & b_2\varrho^{l-2} \cdots \\ 0 & b_0\varrho^l & b_1\varrho^{l-1} \cdots \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot\;\cdot \end{matrix}\right\} k \text{ Zeilen;}$$

darunter stellen wir zunächst die übrigen $(n-l)$ Zeilen mit den a und zum Schlusse die übrigen $(m-k)$ Zeilen mit den b. Nun theilen wir die Determinante in vier Theile nach dem Schema

$$\pm R = \begin{vmatrix} S_1 & S_2 \\ S_3 & S_4 \end{vmatrix} \begin{matrix} (k+l \text{ Zeilen}) \\ (m+n-k-l \text{ Zeilen}) \end{matrix}$$
$$(k+l \text{ Spalten}), \quad (m+n-k-l \text{ Spalten}).$$

In den ersten l Spalten von S_3 stehen überhaupt nur Nullen; in jeder $(l+\alpha)^{\text{ten}}$ Spalte von S_3 ist die niedrigste, in den einzelnen Elementen vorkommende Potenz von ϱ die $(k-\alpha+1)^{\text{te}}$; ihre Glieder enthalten gegen die entsprechenden Elemente einer beliebigen Spalte von S_4 mindestens den Factor $\varrho^{k-\alpha+1}$ mehr. Die Elemente jeder $(l+\alpha)^{\text{ten}}$ Spalte von S_1 enthalten höchstens den Factor $\varrho^{k-\alpha}$. Die Glieder von S_2 enthalten ϱ überhaupt nicht.

Wir berechnen nun R nach dem Laplace'schen Determinantenzerlegungssatze

$$\pm R = S_1 S_4 \pm S_1' S_4' \pm S_1'' S_4'' \pm \cdots,$$

wobei $S_1' S_4'$; $S_1'' S_4''$; $\cdots$ aus $S_1 S_4$ dadurch abgeleitet werden, dass man eine oder mehrere Spalten aus S_1 durch solche aus S_2 und gleichzeitig die unter den letzteren stehenden von S_4 durch die unter den ersteren stehenden von S_3 ersetzt. Wählt man aus S_1 z. B. die $(l+\alpha)^{\text{te}}$ Spalte und ersetzt sie durch eine solche aus S_2, so wird jedes Glied von S_1' hinsichtlich der vorkommenden Potenz von ϱ höchstens um den Factor $\varrho^{k-\alpha}$ erniedrigt; jedes Glied in S_4' dagegen mindestens um den Factor $\varrho^{k-\alpha+1}$ erhöht. Es folgt, dass die Glieder in R mit der niedrigsten Potenz von ϱ sämmtlich in $S_1 S_4$ vorkommen.

Als Glieder mit niedrigster Potenz von ϱ enthält S_1 solche mit ϱ^0. Diese erhält man sämmtlich, wenn man in S_4 einfach $\varrho = 0$ setzt. Dadurch geht S_4 in die Determinante aus

$$\left.\begin{matrix} a_k & a_{k+1} & a_{k+2} & \cdots \\ 0 & a_k & a_{k+1} & \cdots \\ . & . & . & . \end{matrix}\right\} (n - l \text{ Zeilen})$$

$$\left.\begin{matrix} b_l & b_{l+1} & b_{l+2} & \cdots \\ 0 & b_l & b_{l+1} & \cdots \\ . & . & . & . \end{matrix}\right\} (m - k \text{ Zeilen})$$

über, d. h. wenn wir

(5) $a_k + a_{k+1}t + \cdots + a_m t^{m-k} = \psi_1(t), \quad b_l + b_{l+1}t + \cdots + b_n t^{n-l} = \psi_2(t)$

setzen, in die Resultante

$$R_{\psi_1, \psi_2}.$$

Bei S_1 ist gleichfalls das Resultat leicht zu erkennen. Denken wir uns für $a_{k+1}, a_{k+2}, \cdots; b_{l+1}, b_{l+2}, \cdots$ in S_1 eingesetzt $a_{k+1}\varrho^{-1}$, $a_{k+2}\varrho^{-2}, \cdots; b_{l+1}\varrho^{-1}, b_{l+2}\varrho^{-2}, \cdots$, so entsteht eine isobarische Function des Gewichtes kl. Diejenigen ihrer Glieder, welche ein a_{k+1}, $a_{k+2}, \cdots; b_{l+1}, b_{l+2}, \cdots$ besitzen, haben dabei Factoren mit negativen Exponenten von ϱ; es haben daher die in diese Glieder eintretenden Factoren, die von $a_{k+1}, \cdots; b_{l+1}, \cdots$ frei sind, für sich genommen höhere Potenzen von ϱ als die $(k \cdot l)^{\text{te}}$. In S_1 haben deswegen diejenigen Glieder das Minimalgewicht $k \cdot l$, welche $a_{k+1}, a_{k+2}, \cdots; b_{l+1}, b_{l+2}, \cdots$ gar nicht enthalten. Diese bilden demnach, wenn

(6) $a_0 + a_1 t + \cdots + a_k t^k = \varphi_1(t), \quad b_0 + b_1 t + \cdots + b_l t^l = \varphi_2(t)$

gesetzt wird, die Resultante

$$R_{\varphi_1, \varphi_2}.$$

Die Resultante der beiden Gleichungen (4) enthält nur Glieder, die mit $\varrho^{kl}, \varrho^{kl+1}, \cdots$ multiplicirt sind. Die mit ϱ^{kl} multiplicirten haben als Gesammtcoefficienten das Product der beiden Resultanten

(7) $$R_{\varphi_1, \varphi_2} \cdot R_{\psi_1, \psi_2},$$

wobei die Functionen φ und ψ durch (6) und (5) definirt sind. Oder auch: Entwickelt man die Resultante

(8) $$\begin{vmatrix} a_0\varrho^k & a_1\varrho^{k-1} & \cdots & a_{k-1}\varrho & a_k & a_{k+1} & \cdots & a_m & 0 \\ . & . & . & . & . & . & . & . & . \\ b_0\varrho^l & b_1\varrho^{l-1} & \cdots & b_{l-1}\varrho & b_l & b_{l+1} & \cdots & b_n & 0 \\ . & . & . & . & . & . & . & . & . \end{vmatrix}$$

nach steigenden Potenzen von ϱ, so ist das Anfangsglied

$$R_{\varphi_1, \varphi_2} \cdot R_{\psi_1, \psi_2}\varrho^{kl}.$$

Hieraus findet man sofort, indem man statt ϱ einsetzt ϱ^{-1}: Entwickelt man die Resultante

$$(9)\qquad \begin{vmatrix} a_0 & a_1\varrho & \cdots & a_{k-1}\varrho^{k-1} & a_k\varrho^k & a_{k+1}\varrho^k & \cdots & a_m\varrho^k & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_0 & b_1\varrho & \cdots & b_{l-1}\varrho^{l-1} & b_l\varrho^l & b_{l+1}\varrho^l & \cdots & b_n\varrho^l & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

nach fallenden Potenzen von ϱ, dann ist das Anfangsglied

$$R_{\varphi_1, \varphi_2} \cdot R_{\psi_1, \psi_2} \cdot \varrho^{mn-(m-k)(n-l)}.$$

Ordnet man (8) derart, dass die von ϱ freien Glieder vorn stehen und dann die Elemente nach steigenden Potenzen von ϱ geordnet folgen, so sieht man: Die Entwickelung der Resultante

$$(10)\qquad \begin{vmatrix} a_0 & a_1 & \cdots & a_{m-k} & a_{m-k+1}\varrho^1 & \cdots & a_m\varrho^k & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_0 & b_1 & \cdots & b_{n-l} & b_{n-l+1}\varrho^1 & \cdots & b_n\varrho^l & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

nach steigenden Potenzen von ϱ beginnt mit

$$R_{\sigma_1, \sigma_2} \cdot R_{\tau_1, \tau_2} \cdot \varrho^{kl},$$

wobei zu setzen ist

$$\sigma_1(t) = a_0 + a_1 t + \cdots + a_{m-k} t^{m-k}, \quad \sigma_2(t) = b_0 + b_1 t + \cdots + b_{n-k} t^{n-k};$$
$$\tau_1(t) = a_{m-k} + a_{m-k+1} t + \cdots + a_m t^k, \quad \tau_2(t) = b_{n-l} + b_{n-l+1} t + \cdots + b_{n-l} t^{n-l}.$$

§ 367. Wir gehen jetzt zu den beiden Functionen (1) zurück und nehmen an, dass $f_1 = 0$ die $\varkappa$-fache Wurzel (ζ_1, ζ_2) besitze, und dass (ζ_1, ζ_2) zugleich λ-fache Wurzel von $f_2 = 0$ sei. Ohne Beschränkung können wir annehmen, (ζ_1, ζ_2) sei $= (0, 0)$. Dann verschwinden in f_1 alle Coefficienten $a_{\mu,\nu}$, in denen $\mu + \nu < \varkappa$, und in f_2 alle Coefficienten $b_{\mu,\nu}$, in denen $\mu + \nu < \lambda$ ist. Bilden wir unter diesen Festsetzungen $R(z)$, so entsteht eine Determinante, bei deren Elementen wir nur die niedrigsten Potenzen von z_2 aufschreiben, die übrigen Theile dieser Elemente aber unterdrücken wollen. Man erhält dann

$$\begin{vmatrix} a_{m,0}, & a_{m-1,0}, & \cdots & a_{\varkappa,0}, & a_{\varkappa-1,1} z_2, & a_{\varkappa-2,2} z_2^2, & \cdots & a_{0,\varkappa} z_2^{\varkappa}, & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{n,0}, & b_{n-1,0}, & \cdots & b_{\lambda,0}, & b_{\lambda-1,1} z_2, & b_{\lambda-2,2} z_2^2, & \cdots & b_{0,\lambda} z_2^{\lambda}, & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Auf diese Determinante können wir direct den letzten Satz des vorigen Paragraphen anwenden und erkennen daraus, dass in $R(z_2)$ die niedrigste Potenz von z_2 die $(\varkappa \cdot \lambda)^{\text{te}}$ ist. Ein Hinweis auf die Liouville'sche Transformation genügt, um zu zeigen, dass $(0, 0)$ eine $(\varkappa \cdot \lambda)$-fache Wurzel des Systems (1) werden wird.

Die beiden Möglichkeiten, unter denen die Potenz von z_2 eine

höhere werden kann, sind ihrer Bedeutung nach leicht zu unterscheiden. Die erste Möglichkeit tritt ein, wenn

$$a_{m0} z_1^{m-\varkappa} + a_{m-1,0} z_1^{m-\varkappa-1} + \cdots + a_{\varkappa,0} = 0,$$
$$b_{n0} z_1^{n-\lambda} + b_{n-1,0} z_1^{n-\lambda-1} + \cdots + b_{\lambda,0} = 0$$

eine Wurzel gemeinsam haben; die zweite, wenn dies bei

$$a_{\varkappa 0} z_1^{\varkappa} + a_{\varkappa-1,1} z_1^{\varkappa-1} + \cdots + a_{0\varkappa} = 0,$$
$$b_{\lambda 0} z_1^{\lambda} + b_{\lambda-1,1} z_1^{\lambda-1} + \cdots + b_{0\lambda} = 0$$

eintritt.

§ 368. Nach den bisherigen Darlegungen macht es keinen wesentlichen Unterschied, ob $f_1 = 0$, $f_2 = 0$ genau $m \cdot n$ oder weniger Wurzeln besitzen, sobald man nur den Begriff von unendlich grossen Wurzeln zulässt.

Anders ist es jedoch, wenn $f_1 = 0$, $f_2 = 0$ mehr als $m \cdot n$ Wurzeln haben. Dann muss natürlich $R(z_2)$ identisch verschwinden. Es fragt sich, was dies bedeutet. Die beiden Functionen f_1 und f_2 mögen durch eine geeignete Transformation präparirt sein; wir suchen ihren gemeinsamen Theiler. Gesetzt, ein solcher existirte nicht, dann könnte man

$$f_1(z_1, z_2)\, P(z_1, z_2) - f_2(z_1, z_2)\, Q(z_1, z_2) = \varphi(z_2)$$

bestimmen, wobei P von geringerem Grade in z_1 ist als f_2, und Q von geringerem als f_1. Wählt man nun ein $z_2 = \zeta_2$, für welches $\varphi(\zeta_2) \neq 0$ ist, so können wir, weil wegen $R(z_2) \equiv 0$ zu jedem z_2 ein z_1 besteht, welches mit jenem zusammen eine Wurzel von $f_1 = 0$, $f_2 = 0$ ausmacht, durch passendes (ζ_1, ζ_2) die linke Seite zum Verschwinden bringen, während die rechte von Null verschieden bleibt. Dieser Widerspruch fällt nur dann fort, wenn φ identisch Null ist. Dann hat aber, wegen der Grade von P und Q, die Function f mit g einen Factor gemeinsam vgl. § 344. Die Umkehrung des Satzes ist klar. Wir sehen: Die Existenz eines gemeinsamen Theilers von $f_1(z_1, z_2)$ und $f_2(z_1, z_2)$ ist charakteristisch dafür, dass $f_1 = 0$ und $f_2 = 0$ mehr als $m \cdot n$ und zwar unendlich viele Wurzeln haben.

Fünfunddreissigste Vorlesung.

Die Minding'sche Regel. Das Labatie'sche Theorem.

§ 369. Wie wir gesehen haben, führt die Aufstellung der Eliminante zur richtigen Anzahl der Wurzeln zweier Gleichungen mit zwei Unbekannten, oder genauer: zur Anzahl der endlichen Wurzeln. Allein die Durchführung der dazu nothwendigen Rechnungen wird selbst bei

niederen Graden der beiden Gleichungen von so ausserordentlicher Umständlichkeit, dass die Anwendung dieser theoretisch vollkommenen Methode bei einem praktisch vorliegenden Einzelfalle kaum in Erwägung zu ziehen ist. Man müsste sich deshalb, wenn weitere Hülfsmittel nicht zu erlangen sind, im Allgemeinen darauf beschränken, das Maximum der Anzahl von Wurzeln anzugeben, trotzdem diese Anzahl bei weitem zu hoch sein kann.

Diesen Uebelständen wird durch eine von Minding*) gegebene Regel abgeholfen, zu deren Ableitung wir jetzt übergehen wollen. Dieselbe fordert aber einige tiefergehende Vorbereitungen, die sich auf Reihenentwickelung von Wurzeln algebraischer Gleichungen beziehen.

Es sei eine ganz beliebige algebraische Gleichung zwischen den beiden Variablen x und y gegeben

$$f(x, y) = 0, \tag{1}$$

in welcher x bis zum Grade a aufsteigen möge. Zu jedem Werthe von y gehören a Wurzeln x von (1); diese sind nach § 355 stetige Functionen von y. Wir wollen annehmen, dass y über alle Grenzen hinaus wachse, und wollen das Verhalten der a zugehörigen Wurzeln x untersuchen. Kommen in (1) Glieder mit gleichen Potenzen von x aber ungleichen Potenzen von y vor, dann braucht man für den ersten Schritt unserer Untersuchung nur dasjenige von diesen Gliedern beizubehalten, welches die höchste Potenz von y besitzt. Unterdrückt man die übrigen, so reducirt sich (1) auf eine Function von höchstens $(a + 1)$ Gliedern. Wir schreiben das so reducirte Polynom in der Form

$$\varphi(x, y) = Ay^{\alpha}x^{a} + By^{\beta}x^{b} + Cy^{\gamma}x^{c} + \cdots + Ly^{\lambda}x^{l}, \tag{2}$$
$$(a > b > c > \cdots > l \geq 0).$$

Die Darstellung von x als Function von y soll nun durch eine nach absteigenden Potenzen von y geordnete Reihe geliefert werden. In ihr sei uy^{ϱ} das Glied höchster Potenz in y. Wir nennen es das Leitglied der Entwickelung, und ϱ möge die Ordnung des zugehörigen x heissen. Setzen wir dies in (2) ein, so werden sich die Glieder höchster Potenzen von y zerstören müssen. Es müssen deshalb mindestens zwei Glieder höchster Ordnung gleichzeitig auftreten, wenn uy^{ϱ} wirklich das Leitglied einer Entwickelung abgiebt. Die Werthe von ϱ können demnach nur solche sein, bei denen unter den Grössen

---

*) Bestimmung des Grades einer durch Elimination hervorgehenden Gleichung. J. f. M. Bd. 22 (1841), p. 178. — Entwickelung eines symmetrischen Ausdrucks für den Grad einer durch Elimination hervorgehenden Gleichung. J. f. M. Bd. 31 (1846), p. 1.

$$(3) \qquad \alpha + a\varrho, \quad \beta + b\varrho, \quad \gamma + c\varrho, \cdots \lambda + l\varrho$$

mindestens zwei vorhanden sind, deren Werthe übereinstimmen, und deren Werth zugleich von keinem anderen der Reihe (3) übertroffen wird. Setzt man zwei dieser Grössen einander gleich, z. B. $(\mu + m\varrho)$ und $(\nu + n\varrho)$, so folgt

$$(4) \qquad \varrho = \frac{\nu - \mu}{m - n},$$

und es wird der gemeinsame Werth jener beiden Grössen

$$(5) \qquad \mu + m\varrho = \nu + n\varrho = \frac{m\nu - n\mu}{m - n}.$$

Gefordert ist dann, dass dieser von keinem andern aus (3)

$$(6) \qquad \varkappa + k\varrho = \frac{\varkappa(m - n) + k(\nu - \mu)}{m - n}$$

übertroffen werde. Ist dies der Fall, dann giebt (4) eine passende Ordnung für die Entwickelung von x.

§ 370. Am einfachsten lassen sich diese Verhältnisse übersehen, wenn wir von einer geometrischen Darstellung Gebrauch machen, welche Newton angegeben hat, und die den Namen des Newton'schen Polygons führt*).

In einer Hülfsebene ziehen wir zwei senkrecht auf einander stehende Axen, deren eine, etwa die horizontale, zur Darstellung der Exponenten von x, und deren andere, die verticale, zur Darstellung der Exponenten von y dienen soll. Jedes der Werthepaare (a, α), (b, β), (c, γ), $\cdots (l, \lambda)$ wird dann durch einen Punkt der Ebene repräsentirt. Die Gerade, welche die Punkte (m, μ) und (n, ν) mit einander verbindet, hat, wenn ξ und η ihre laufenden Coordinaten bedeuten, die Gleichung

$$(7) \qquad \eta + \frac{\nu - \mu}{m - n}\xi = \frac{m\nu - n\mu}{m - n};$$

sie schneidet aus der durch $(k, \varkappa)$ gehenden Senkrechten zur x-Axe das Stück

$$\eta_0 = \frac{m\nu - n\mu}{m - n} + k\frac{\mu - \nu}{m - n}$$

heraus, und die Erhebung des Schnittpunktes (k, η_0) über $(k, \varkappa)$ beträgt, mit dem richtigen Vorzeichen genommen,

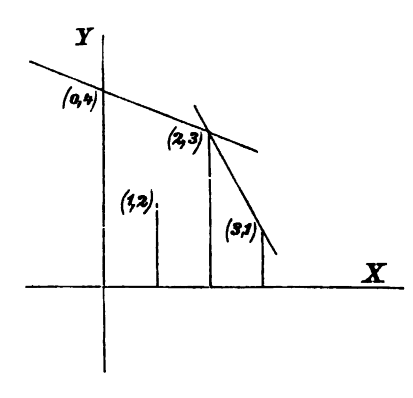
$$\frac{m\nu - n\mu}{m - n} - \frac{\varkappa(m - n) + k(\nu - \mu)}{m - n}.$$

Die Vergleichung dieses Werthes mit (5) und (6) zeigt, dass $\frac{\nu - \mu}{m - n}$

*) Newton, Opuscula; ed. Castillon, p. 12 u. 39. — Vgl. hierüber, sowie über die Entwickelung des x nach fallenden Potenzen auch C. Jordan, Cours d'analyse I, p. 89 ff.

nur dann ein als Exponenten des Leitgliedes brauchbares ϱ liefern kann, wenn die gerade Linie, welche die Punkte (m, μ) und (n, ν) mit einander verbindet, keinen der übrigen Punkte (a, α), (b, β), $\cdots$ vom Nullpunkte trennt.

Hiernach liefert eine einfache Zeichnung sofort alle überhaupt für ϱ möglichen Werthe. Jedenfalls geht durch den äussersten nach rechts gelegenen Punkt (a, α) eine der Geraden des Newton'schen Polygons. Der äusserste auf ihr nach links hin gelegene zu (2) gehörige Punkt sei etwa (d, δ). Dann kann, wie geometrisch klar ist, keine weitere Polygonseite durch einen der zwischen (a, α) und (d, δ) liegenden Systempunkt von (2) laufen. Dagegen muss durch (d, δ) eine zweite Gerade der angegebenen Art gezogen werden können; diese wird eine geringere Steigung besitzen, als die erste, so dass das zu ihr gehörige ϱ geringer ist, als das zur ersten Seite gehörige. In ähnlicher Weise kann man fortgehen, bis man zum linken Endpunkt des Polygons kommt, welcher auf der Verticalaxe liegt. Die letzte Seite liefert das kleinste ϱ.



Die Entfernung der Fusspunkte von (m, μ) und (n, ν) wollen wir die Horizontalcomponente der zugehörigen Seite nennen. Die Summe aller Horizontalcomponenten ist gleich dem Grade in x.

Nach dem Dargelegten erklärt sich die Figur, welche zu

$$f(x, y) = (y - 1)x^3 + y^3x^2 + (2y^3 - 2y)x + (y^4 - y^2 + 1),$$
$$\varphi(x, y) = yx^3 + y^3x^2 + 2y^3x + y^4$$

gehört, von selbst. Sie liefert

$$1 + 3\varrho = 3 + 2\varrho; \qquad \varrho = 2,$$
$$3 + 2\varrho' = 4 + 0\varrho'; \qquad \varrho' = \frac{1}{2},$$
$$x = uy^2 \quad \text{und} \quad x = u'y^{\frac{1}{2}}.$$

§ 371. Wir wollen nun annehmen, es würden durch $x = uy^\varrho$ die beiden unmittelbar aufeinander folgenden Glieder aus (3)

$$(8) \qquad \mu + m\varrho \quad \text{und} \quad \nu + n\varrho \qquad (m = n + 1)$$

einander gleich und grösser als die übrigen derselben Reihe. Das ergäbe also $\varrho = (\nu - \mu)$, und es sind sämmtliche anderen Exponenten

$$(9) \quad \alpha + a(\nu - \mu), \quad \beta + b(\nu - \mu), \; \cdots \; \text{kleiner als} \; \mu + m(\nu - \mu).$$

Wir tragen nun in (1) ein

$$(10)\qquad x = uy^\varrho + x_1 \qquad (\varrho = \nu - \mu).$$

Um das Resultat bequem übersehen zu können, machen wir die Substitution in den beiden durch (8) angedeuteten Gliedern

$$M(uy^\varrho + x_1)^m y^\mu, \quad N(uy^\varrho + x_1)^n y^\nu \qquad (M, N \neq 0)$$

und einem die sämmtlichen übrigen Glieder repräsentirenden Term

$$D(uy^\varrho + x_1)^d y^\delta.$$

Wir erhalten diesen dreien entsprechend als transformirte Glieder ohne x_1

$$(11)\qquad \begin{matrix} Mu^m y^{\mu+m\varrho}; \quad Nu^n y^{\nu+n\varrho}, \\ Du^d y^{\delta+d\varrho}, \end{matrix} \qquad (m = n+1;\ \varrho = \nu - \mu).$$

Wegen (8), (9) haben die beiden ersten einen höheren Grad in y als alle anderen, welche um mindestens eine Einheit zurückstehen. Setzt man

$$(12)\qquad Mu + N = 0, \quad u = -\frac{N}{M},$$

dann zerstören sich jene beiden und ein Glied der dritten Art bleibt als höchstes zurück. u soll diesen Werth (12) annehmen.

Als Glieder, die $x_1^{\,1}$ enthalten, finden wir in den Gliedern (11)

$$\begin{matrix} Mmu^{m-1} y^{\mu+(m-1)\varrho} x_1, \quad Nnu^{n-1} y^{\nu+(n-1)\varrho} x_1, \\ Ddu^{d-1} y^{\delta+(d-1)\varrho} x_1. \end{matrix} \qquad (m = n+1;\ \varrho = \nu - \mu).$$

Die beiden ersten liefern gleiche, und zwar die höchsten Potenzen in y. Ihr Aggregat kann nicht verschwinden, da sonst wegen (12) auch M und N gleich 0 wären.

Als Glieder mit $x_1^{\,2}$ werden ebenso gefunden,

$$\begin{matrix} M\binom{m}{2} u^{m-2} y^{\mu+(m-2)\varrho} x_1^{\,2}, \quad N\binom{n}{2} u^{n-2} y^{\nu+(n-2)\varrho} x_1^{\,2}, \\ D\binom{d}{2} u^{d-2} y^{\delta+(d-2)\varrho} x_1^{\,2}. \end{matrix} \qquad (m = n+1;\ \varrho = \nu - \mu).$$

Auch hier erkennt man sofort, dass die beiden ersten Glieder unter allen denen mit $x_1^{\,2}$ die höchsten Grade in y liefern.

Beim Newton'schen Polygon der Gleichung in x_1 und y kommen also für den Abschluss links drei Systempunkte in Frage

$$(13)\quad (0,\ \delta + d\varrho); \quad (1,\ \mu + (m-1)\varrho); \quad (2,\ \mu + (m-2)\varrho).$$

Bestimmt man demgemäss $x_1 = u_1 y^{\varrho_1}$, so kommen als kleinste Werthe von ϱ_1 in Betracht die, für welche

$$\varrho_1 + \mu + (m-1)\varrho = \delta + d\varrho \quad \text{d. h.} \quad \varrho_1 = (\delta + d\varrho) - (\mu + m\varrho) + \varrho$$

und an zweiter Stelle die, für welche

$$2\varrho_1 + \mu + (m-2)\varrho = \mu + (m-1)\varrho \quad \text{d. h.} \quad \varrho_1 = \varrho$$

ist. Daraus folgt: Die letzte Polygonseite verbindet die beiden ersten

Systempunkte (13); sie liefert wegen (9) ein $\varrho_1 < \varrho$. Die vorhergehende Seite liefert ein ϱ_1, welches mindestens $= \varrho$ ist. Da nun eine Weiterentwickelung $x = uy^{\varrho} + u_1 y^{\varrho_1} + x_2$ nur dann einen Sinn hat, wenn $\varrho_1 < \varrho$ hat, so erkennt man, dass diese Entwickelung nur auf eine einzige Art mit einem ganzzahligen $\varrho_1 < \varrho$ fortgeführt werden kann.

Macht man die Substitution $x = uy^{\varrho} + u_1 y^{\varrho_1} + x_2$ in (1), dann wiederholen sich alle besprochenen Schlüsse. Ferner ist aber ersichtlich, dass durch unsere neue Transformation gegen (10) keine höheren Grade in y eingeführt werden; man braucht nur $x_1 = u_1 y^{\varrho_1} + x_2$ in die transformirte Gleichung zu setzen, um das einzusehen. Bei passender, der Annahme (12) entsprechender Wahl kann man das nunmehr höchste Glied in y tilgen, u. s. f. So folgt: Durch eine Substitution

$$(14) \qquad x = uy^{\varrho} + u_1 y^{\varrho_1} + u_2 y^{\varrho_2} + \cdots + u_\lambda y^{\varrho_\lambda}$$

ist es möglich, die Gleichung $f(x, y) = 0$ bis auf Glieder zu befriedigen, die in y von niederer als der r^{ten} Potenz sind, wobei r eine beliebig hohe negative Zahl bedeutet; oder auch: durch die Substitution

$$(15) \qquad x = uy^{\varrho} + u_1 y^{\varrho_1} + u_2 y^{\varrho_2} + \cdots + u_\lambda y^{\varrho_\lambda} + x_{\lambda+1}$$

geht $f(x, y)$ in ein $f_{\lambda+1}(x_{\lambda+1}, y)$ über, welches nur Potenzen $y^{-r-1}, y^{-r-2}, \cdots$ in endlicher Anzahl besitzt.

§ 372. Wir gehen nun zu dem allgemeinsten Falle über. Eine Seite des Newton'schen Polygons möge sich vom Punkte (m, μ) bis zum Punkte (n, ν) von rechts nach links erstrecken, und zwar möge $m = (n + \sigma)$ sein. Wenn ferner $x = uy^{\varrho}$ eingesetzt wird, sollen die auf dieser Seite liegenden Eckpunkte die höchsten Potenzen von y aufweisen. Es muss also

$$(8^*) \quad m\varrho + \mu = n\varrho + \nu, \quad \varrho = \frac{\nu - \mu}{\sigma} = \frac{p}{q} \quad (\nu - \mu = p\tau, \ \sigma = q\tau)$$

sein, wobei $\frac{p}{q}$ die kleinste Benennung des Bruches ϱ angiebt. Kommt zwischen den beiden Grenzpunkten der Seite noch ein anderer Systempunkt (m', μ') auf ihr vor, so ist

$$m\varrho + \mu = m'\varrho + \mu'; \qquad (m - m')p = (\mu' - \mu)q,$$

und da p und q theilerfremd sind, so muss es eine ganze Zahl h geben, für welche

$$m' = m - hq, \qquad \mu' = \mu + hp$$

wird. Die höchsten Potenzen von y werden also durch Glieder

$$(16) \quad Mx^m y^\mu + M'x^{m-q} y^{\mu+p} + M''x^{m-2q} x^{\mu+2p} + \cdots + Nx^{m-q\tau} y^{\mu+p\tau}$$

geliefert. Die übrigen Systempunkte mögen generell durch

$$Dx^d y^\delta$$

bezeichnet werden. Jetzt machen wir die Substitution

(10^a) $$x = uy^{\varrho} + x_1 \quad \left(\varrho = \frac{p}{q}\right)$$

und erhalten als transformirte Glieder ohne x_1

(11^a) $$Mu^m y^{\mu+\varrho m}, \quad M'u^{m-q} y^{\mu+\varrho m}, \quad \ldots, \quad Nu^{m-q\tau} y^{\mu+\varrho m}, \\ Du^d y^{\delta+\varrho d},$$

als solche mit x_1^1

(11^b) $$Mmu^{m-1} y^{\mu+\varrho(m-1)} \cdot x_1, \quad M'(m-q)u^{m-q-1} y^{\mu+\varrho(m-1)} \cdot x_1, \ldots \\ Ddu^{d-1} y^{\delta+\varrho(d-1)} x_1,$$

u. s. w. Dabei ist

(17) $$\mu + \varrho m > \delta + \varrho d, \quad \mu + \varrho(m-1) > \delta + \varrho(d-1), \cdots.$$

Das Aggregat der ersten Glieder in (11^a) wird verschwinden, wenn u eine Wurzel der Gleichung

(12^a) $$Mu^{\tau q} + M'u^{(\tau-1)q} + M''u^{(\tau-2)q} + \cdots + N = 0$$

ist. Man überzeugt sich sofort davon, dass für eine k-fache Wurzel von (12^a) auch die zu (16) gehörigen Glieder mit x_1, x_1^2, $\cdots x_1^{k-1}$ verschwinden, während die mit x_1^k von Null verschieden bleiben. Giebt man dem u in (10^a) alle Wurzelwerthe von (12^a) und rechnet jeden in der Multiplicität, mit welcher er als Wurzel auftritt, dann giebt es $\tau q = \sigma$ Entwickelungsmöglichkeiten (10^a) von x, bei denen die Seite von (m, μ) bis (n, ν) das leitende Glied liefert. Führt man dies Verfahren bei allen übrigen Polygonseiten durch, so kommt man zu genau so vielen Entwickelungsanfängen, als der Grad von (1) in x angiebt.

§ 373. Wir legen jetzt eine k-fache Wurzel von (12^a) den weiteren Betrachtungen zu Grunde.

Es werden dann, wenn wir (1) durch (10^a) transformiren, in dem neuen Polynome $f_1(x_1, y)$ aus dem Aggregate der zu $(m, \mu) \cdots (n, \nu)$ gehörigen Glieder diejenigen verschwinden, welche mit $x_1^0, x_1^1, \cdots x_1^{k-1}$ multiplicirt vorkommen würden; dagegen ist der Coefficient des mit x_1^k multiplicirten Gliedes von Null verschieden. Es sind die Coefficienten, wenn man die höchsten Glieder in y heraushebt, von

x_1^0 gleich $Du^d \cdot y^{\delta+\varrho d}$;

x_1^{k-1} gleich $D\binom{d}{k-1} u^{d-k+1} \cdot y^{\delta+\varrho(d-k+1)}$;

x_1^k gleich $\left(M\binom{m}{k} u^{m-k} + M'\binom{m'}{k} u^{m'-k} + \cdots\right) \cdot y^{\mu+\varrho(m-k)}$;

x_1^{k+1} gleich $\left(M\binom{m}{k+1} u^{m-k-1} + M'\binom{m'}{k+1} u^{m'-k-1} + \cdots\right) \cdot y^{\mu+\varrho(m-k-1)}$,

oder, wenn dieses Glied verschwindet,

$$\text{gleich} \quad D\binom{d}{k+1} u^{d-k+1} \cdot y^{\delta+\varrho(d-k-1)}.$$

Würde eine Seite des Newton'schen Polygons nach ihrer Horizontalcomponente von $(k+1)$ bis (k) gehen, dann müsste in $x_1 = u_1 y^{\varrho_1}$
$\varrho_1(k+1) + \mu + \varrho(m-k-1) = \varrho_1 k + \mu + \varrho(m-k)$ d. h. $\varrho_1 = \varrho$
oder bei Eintreten der zweiten eben erwähnten Eventualität
$\varrho_1(k+1) + \delta + \varrho(d-k-1) = \varrho_1 k + \mu + \varrho(m-k)$ d. h. $\varrho_1 > \varrho$
gesetzt werden, wie aus (17) folgt, da ja hier

$$\varrho_1 = \varrho + [(\mu + \varrho m) - (\delta + \varrho d)]$$

sein würde. Machen wir die gleiche Substitution, um die Steigung der Polygonseite zu erhalten, deren Horizontalcomponente von (k) bis $(k-\alpha)$ geht, $(\alpha = 1, 2, \cdots k)$, so ist zu setzen
$\varrho_1 k + \mu + \varrho(m-k) = \varrho_1(k-\alpha) + \delta + \varrho(m-k+\alpha)$ d. h. $\varrho_1 < \varrho$,
da ja hier

$$\varrho_1 = \varrho - \frac{1}{\alpha}[(\mu + \varrho m) - (\delta + \varrho d)] \tag{18}$$

sein wird. Dies zeigt, dass eine Seite des Polygons ihren linken Endpunkt in $(k, \mu + \varrho(m-k))$ hat, und dass die links davon liegenden Seiten, deren Horizontalcomponenten zusammen k betragen, sämmtlich durch Substitutionen $x_1 = u_1 y^{\varrho_1}$ befriedigt werden, bei denen $\varrho_1 < \varrho$ ist.

Den Schlusssätzen des vorigen Paragraphen gemäss giebt es also k und auch nur k Entwickelungen $x = uy^{\varrho} + u_1 y^{\varrho_1}$, bei denen $\varrho_1 < \varrho$ wird. Das ist so zu denken, dass für die Horizontalcomponente von (k) bis (0) entweder k Seiten bestehen von der Länge 1 der Horizontalcomponente, oder auch weniger Seiten mit grösserer Horizontalausdehnung. Wir wollen allgemein annehmen, dass eine der Seiten betrachtet werde, welche von (m_1) bis $(m_1 - \sigma_1)$ sich erstreckt. Dabei ist natürlich $\sigma_1 \leqq k \leqq \tau$; denn (12^a^) kann Wurzeln höchstens in der τ-fachen Multiplicität besitzen. Das zugehörige ϱ_1 wird nach (18) den Nenner σ_1 haben; wir setzen es, auf seine kleinste Benennung gebracht,

$$\varrho_1 = \frac{p_1}{q_1}; \quad \sigma_1 = q_1 \tau_1, \quad \text{also} \quad q q_1 \tau_1 < q\tau = \sigma \leqq a. \tag{19}$$

Von hier ab wiederholen sich die früheren Schlüsse. Der Werth von u_1 wird durch eine Gleichung bestimmt werden, welche der Gleichung (12^a^) entspricht,

$$M_1 u_1^{\tau_1 q_1} + M_1' u_1^{(\tau_1 - 1) q_1} + \cdots + N_1 = 0, \tag{12^b}$$

bei der die Multiplicität einer Wurzel die Ordnung τ_1 nicht übertreffen kann, u. s. w.

Transformirt man dann $f_1(x_1, y)$ durch

$$x_1 = u_1 y^{\varrho_1} + x_2,$$

so kommt man zu $f_2(x_2, y)$ u. s. f. Die neue Substitution $x_2 = u_2 y^{\varrho_2}$

führt auf $\varrho_2 < \varrho_1$; bringt man ϱ_2 auf die kleinste Benennung $p_2 : q_2$ und setzt $q \cdot q_1 \cdot q_2$ an, so wird dies wieder $\leqq a$, u. s. f. So folgt, dass die Nenner $q, q_1, q_2, \cdots$ nicht alle grösser als 1 sein können. Von einer gewissen Stelle ab werden alle q_λ gleich 1 sein. Führt man

$$y = \eta^{q_1 \cdot q_2 \cdots q_r}$$

in (1) ein, wobei q_r der letzte Nenner ist, der die Einheit übertrifft, so wird

$$f(x, y) = \varphi(x, \eta)$$

werden, derart, dass die Entwickelung der entsprechenden Wurzel von $\varphi = 0$ nur ganze Potenzen von η enthält. Ja, wenn man alle a Entwickelungen in Betracht zieht, kann man

$$y = \eta^Q$$

so bestimmen, dass sämmtliche a Entwickelungen der Wurzeln x von $f(x, \eta^Q) = 0$ nur nach ganzen, abnehmenden Potenzen von η fortschreiten.

Bevor wir diese letzte Eigenschaft bewiesen hatten, war es noch nicht möglich, zu erkennen, dass durch eine Substitution (14) Glieder in y getilgt werden konnten, derart, dass nur niedere Potenzen als y^{-r} vorkommen; denn bei jedem Fortschritte der Substitution hätten durch neue Nenner des ϱ neue Glieder eingeführt werden können, deren Exponenten zwar abnehmen müssen, aber sich doch einer festen Grenze hätten nähern können. Das ist jetzt ausgeschlossen, da kein Exponent einen Nenner $> Q$ haben kann. Der Schlusssatz aus § 371 gilt in jedem Falle.

Nun denken wir uns (1) nach x aufgelöst; die a Wurzeln werden Functionen von y sein; man nennt sie algebraische Functionen. Bezeichnen wir sie mit $\omega_1(y), \omega_2(y), \cdots \omega_a(y)$, so ist

$$(20) \quad f(x, y) = C_0(y) \cdot (x - \omega_1(y))(x - \omega_2(y)) \cdots (x - \omega_a(y)),$$

wenn $C_0(y)$ den Coefficienten von x^a in $f(x, y)$ bedeutet. Entwickelt man ferner alle ω nach fallenden Potenzen von y in Potenzreihen und setzt dies, sowie einen der Werthe (14) in (20) ein, so muss in dem Producte rechts jede Potenz von y, die höher als y^{-r} ist, verschwinden. Also stimmt (14) mit den Entwickelungen eines ω in den ersten Gliedern überein, und diese Uebereinstimmung kann durch Vergrösserung von r beliebig weit getrieben werden. So erkennt man: Die Reihen (14) liefern die Anfangsglieder der Reihenentwickelungen der Wurzeln x von (1).

§ 374. Durch diese Resultate haben wir die Mittel in Händen, die zu Anfang dieser Vorlesung aufgeworfene Frage zu erledigen.

Wir sahen (§ 136, Bd. I), dass die Resultante von

$$f(x) = a_0 z^m + a_1 z^{m-1} + a_2 z^{m-2} + \cdots + a_m,$$
$$g(z) = b_0 z^n + b_1 z^{n-1} + b_2 z^{n-2} + \cdots + b_n$$

durch die Formel bestimmt ist

$$R_{f,g} = a_0^n g(\alpha_1) g(\alpha_2) \cdots g(\alpha_m) = (-1)^{mn} b_0^m f(\beta_1) f(\beta_2) \cdots f(\beta_n),$$

in welcher die α die Wurzeln von $f = 0$, die β die Wurzeln von $g = 0$ bezeichnen.

Wenden wir dies auf die beiden Gleichungen

$$f(x, y) = 0, \quad g(x, y) = 0$$

an, und nennen $x_1, x_2, \cdots x_m$ die Wurzeln x von $f(x, y) = 0$ bei unbestimmten y, und $\xi_1, \xi_2, \cdots \xi_n$ diejenigen von $g(x, y) = 0$; ferner $a_0(y)$ und $b_0(y)$ die höchsten Coefficienten von f und von g, so folgt

$$(21) \qquad \begin{aligned} R_{f,g}(y) &= a_0^n(y) \cdot g(x_1, y) g(x_2, y) \cdots g(x_m, y) \\ &= (-1)^{mn} b_0^m(y) \cdot f(\xi_1, y) f(\xi_2, y) \cdots f(\xi_n, y) \end{aligned}$$

als Eliminante. Hat man die Anfangsglieder der Reihenentwickelungen der x_λ und der ξ_λ nach fallenden Potenzen von y, so giebt jeder der beiden Ausdrücke in (21) ein bequemes Mittel, den Grad von R zu bestimmen, da ja die Gradbestimmung jedes einzelnen Factors ohne Mühe geliefert werden kann. Jeder dieser Grade ist eine ganze oder gebrochene positive Zahl, weil die a_λ in y mindestens den Grad Null haben. Ihre Summe ist eine positive Zahl, welche wegen der Bedeutung von R auch ganz sein muss. Führt man hinlänglich viele Glieder der Entwickelungen ein, so kann man auf diesem Wege sogar die gesammte Eliminante herstellen.

Nehmen wir, um das Verfahren an einem Beispiele zu erläutern, etwa wie in § 370

$$f(x, y) = (y - 1)x^3 + y^3 x^2 + (2y^3 - 2y)x + (y^4 - y^2 + 1),$$

so haben wir dafür

$$x_1 = -y^2 + \cdots, \quad x_2 = \sqrt{-1} \cdot y^{\frac{1}{2}} + \cdots, \quad x_3 = -\sqrt{-1}\, y^{\frac{1}{2}} + \cdots.$$

Hierzu nehmen wir als zweite Function

$$g(x, y) = (y^2 + 1)x^2 + (y^3 - 2y + 3)x + (2y^4 + y - 2),$$

und dann ergiebt sich für die Gradbestimmung von $R_{f,g}(y)$

$$[a_0(y)] = 1; \quad [g(x_1, y)] = 6, \quad [g(x_2, y)] = [g(x_3, y)] = 4,$$
$$[R_{f,g}(y)] = 2 + 6 + 4 + 4 = 16;$$

also tritt gegen das Product der Dimensionen eine Verminderung der Wurzelanzahl um 4 ein.

Wenn wir dasselbe Verfahren auf $R_{f,g}(x)$ anwenden, ergiebt sich

$$f(x,y) = y^4 + x^2y^3 + (2x-1)y^2 + (x^3-2x)y + (-x^3+1),$$

$$y_1 = -x^2 + \cdots,\ y^2 = \sqrt{-1}\cdot x^{\frac{1}{2}} + \cdots,\ y_3 = -\sqrt{-1}\cdot x^{\frac{1}{2}} + \cdots,\ y_4 = 1 + \cdots.$$

$$[a_0(x)] = 0,\ [g(x,y_1) = 8,\ [g(x,y_2)] = [g(x,y_3)] = 3,\ [g(x,y_4)] = 2.$$

$$[R_{f,g}(x)] = 0 + 8 + 3 + 3 + 2 = 16.$$

Im Allgemeinen genügt es, die Werthe der leitenden Exponenten zu kennen, um die Gradzahlen zu bestimmen; doch kann es vorkommen, dass man mehrere Glieder der Entwickelung braucht. Dies tritt ein, wenn in $g(x_\alpha, y)$ durch Einsetzen von $x_\alpha = uy^\varrho$ die höchsten vorkommenden Glieder in y vermöge des besonderen Werthes von u sich zerstören*).

§ 375. Obwohl das angegebene Verfahren hinsichtlich der Leichtigkeit der Rechnung nichts zu wünschen übrig lässt, so führt es doch nicht auf einen Ausdruck, welcher aus den durch beide Gleichungen gelieferten Elementen symmetrisch zusammengesetzt wäre. Ein solcher soll jetzt abgeleitet werden.

Wir gehen dazu auf die Resultantenform (3) aus § 136, Bd. I zurück, setzen statt der α_λ die x_λ, d. h. die Wurzeln von $f(x,y) = 0$ bei unbestimmten y und statt der β_λ die ξ_λ, d. h. die Wurzeln von $g(x,y) = 0$ ein. So kommt

$$\begin{aligned} R_{f,g}(y) = a_0^n(y)\, b_0^m(y)\, &(x_1-\xi_1)(x_1-\xi_2)\cdots(x_1-\xi_n)\\ &(x_2-\xi_1)(x_2-\xi_2)\cdots(x_2-\xi_n)\\ &\quad\cdots\cdots\cdots\cdots\\ &(x_m-\xi_1)(x_m-\xi_2)\cdots(x_m-\xi_n) \end{aligned}$$

heraus, und für die x_λ, ξ_λ tragen wir die Entwickelungen nach fallenden Potenzen in y ein. Dann ist der Grad einer jeden Differenz $(x_\lambda - \xi_\mu)$ durch den Grad desjenigen der Elemente bestimmt, welches

*) Magnus hat J. f. M. Bd. 26, p. 365 die Methode als incorrect angegriffen. Sobald man auf die letzte oben gemachten Bemerkungen achtet, ist sie vollkommen correct. Das von Magnus gegebene Beispiel, bei welchem die Ordnungen unrichtig werden sollen, ist

$$f(x,y) = x^3 - (7y-7)x^2 + (14y^2 - 30y + 7)x - 8y^3 + 20y^2 + 18y - 15 = 0,$$
$$g(x,y) = x^2 - (6y-4)x + 8y^2 - 12y + 5 = 0.$$

Falls man als Wurzeln der ersten Gleichung annimmt

$$x_1 = y + x_1',\qquad x_2 = 2y - 6 + x_2',\qquad x_3 = 4y - 2 + x_3',$$

ergiebt sich richtig

$$[R_{f,g}(y)] = 3.$$

Vgl. J. f. M. 27 (1844), p. 379.

den höheren Grad in y besitzt. Sind x_λ und ξ_μ von gleichem Grade, dann müssen die Entwickelungen so weit getrieben werden, dass $(x_\lambda - \xi_\mu)$ in seinem nicht verschwindenden leitenden Gliede bekannt ist. Es sei

$$[x_\alpha] = r_\alpha, \qquad [\xi_\alpha] = \varrho_\alpha.$$

Die $r_1, r_2, \cdots$, sowie die $\varrho_1, \varrho_2, \cdots$ mögen in eine einzige Reihe von nicht abnehmenden Gliedern eingeordnet sein. Dann sind so viele von den Differenzen $(x_\lambda - \xi_\mu)$ vom Grade r_α, als Grössen $\varrho_1, \varrho_2, \cdots$ vorhanden sind, die kleinere Werthe als r_α haben. Setzen wir also fest, dass k_α bedeuten soll, wie viele unter den Grössen $\varrho_1, \varrho_2, \cdots$ kleiner sind als r_α; und $\varkappa_\alpha$, wie viele unter den Grössen $r_1, r_2, \cdots$ kleiner sind als ϱ_α, (wobei man i. A. für gleiche Grade nach Belieben die r_α den ϱ_α vor- oder nachsetzen kann), dann wird die Gradbestimmung der Eliminante durch die symmetrisch gebaute Formel geliefert

$$[R_{f,g}(y)] = n[a_0(y)] + m[b_0(y)] + \sum k_\alpha r_\alpha + \sum \varkappa_\alpha \varrho_\alpha.$$

In dem von uns oben behandelten Beispiele ist

$$\varrho_1 = 1, \ \varrho_2 = 1; \quad r_1 = 2, \ r_2 = \frac{1}{2}, \ r_3 = \frac{1}{2}; \quad [a_0] = 1;$$

$$\varkappa_1 = 2, \ \varkappa_2 = 2; \quad k_1 = 2, \ k_2 = 0, \ k_3 = 0; \quad [b_0] = 2;$$

$$[R_{f,g}(y)] = 2 \cdot 1 + 3 \cdot 2 + 4 + 2 + 2 = 16.$$

§ 376. Eine Methode der Eliminantenberechnung ist, wie angedeutet wurde, in dem Besprochenen enthalten. Wir wollen hier noch eine andere kurz herleiten, welche von Labatie*) angegeben worden ist. Sie geht von dem Algorithmus der Bestimmung des grössten gemeinsamen Theilers aus. Sind die beiden vorgelegten Gleichungen

$$(22) \qquad f(z_1, z_2) = 0, \quad f_1(z_1, z_2) = 0,$$

dann kann man auf rationalem Wege den grössten gemeinsamen Theiler $f_r(z_1, z_2)$ der beiden Polynome f und f_1 bestimmen und

$$f(z_1, z_2) = \varphi(z_1, z_2) f_r(z_1, z_2); \qquad f_1(z_1, z_2) = \varphi_1(z_1, z_2) f_r(z_1, z_2)$$

ansetzen. Jede Wurzel von $f_r = 0$ ist auch eine Wurzel von (22); neben diese treten die Wurzeln von

$$\varphi = 0, \ f_r = 0 \quad \text{und} \quad \varphi_1 = 0, \ f_r = 0,$$

welche zwar unter jenen schon vorkommen, die aber doch die Multiplicität der betreffenden Wurzeln von $f_r = 0$ beeinflussen; und ferner noch die Wurzeln der beiden Gleichungen

*) Labatie, Méthode d'élimination par le plus grand commun diviseur entièrement rectifiée et appliquée etc. Paris 1835. Bachelier.

$$\varphi(z_1, z_2) = 0, \quad \varphi_1(z_1, z_2) = 0,$$

deren Polynome zu einander theilerfremd sind. Diese bilden natürlich den Haupttheil der Untersuchung, und ihnen wollen wir uns zuwenden, indem wir voraussetzen, dass (22) schon von gemeinsamen Factoren der Polynome befreit wäre.

Wir verwenden die Resultate von § 345. Die dortige Formel (5) giebt

$$\begin{aligned} f &= f_1 q_1 - f_2 \varphi_2, \\ f_1 \psi_1 &= f_2 q_2 - f_3 \varphi_3, \\ f_2 \psi_2 &= f_3 q_3 - f_4 \varphi_4, \\ &\cdots\cdots\cdots \\ f_{r-2} \psi_{r-2} &= f_{r-1} q_{r-1} - \varphi_r, \end{aligned}$$

wobei $f_r = 1$ gesetzt ist. Die $\varphi_2, \varphi_3, \cdots \varphi_r$; $\psi_1, \psi_2, \cdots \psi_{r-2}$ sind ganze Functionen von z_2 allein. Wir können ψ_α und $\varphi_{\alpha+2}$ ohne gemeinsamen Theiler annehmen. Denn haben beide Functionen einen solchen, so hat ihn auch $f_{\alpha+1} q_{\alpha+1}$. Nun sind aber (§ 345) die f_α als derartige Functionen vorausgesetzt, dass sie keinen von z_1 freien Factor besitzen; demnach haben $\psi_\alpha, \varphi_{\alpha+2}, q_{\alpha+1}$ einen gemeinsamen Theiler, und mit diesem kann dann die ganze Gleichung durchdividirt werden. Wir bezeichnen nun den grössten gemeinsamen Theiler von

ψ_1, φ_3	mit	d_1;	$\frac{\psi_1}{d_1}$	und	$\frac{\varphi_3}{d_1}$	sind ganz und theilerfremd
$\frac{\psi_1 \psi_2}{d_1}, \varphi_4$	„	d_2;	$\frac{\psi_1 \psi_2}{d_1 d_2}$	„	$\frac{\varphi_4}{d_2}$	„ „ „ „
$\frac{\psi_1 \psi_2 \psi_3}{d_1 d_2}, \varphi_5$	„	d_3;	$\frac{\psi_1 \psi_2 \psi_3}{d_1 d_2 d_3}$	„	$\frac{\varphi_5}{d_3}$	„ „ „ „
. . . .						

wobei zu bemerken ist, dass wir $d_1 = 1$ hätten setzen können.

Wir entnehmen ferner aus § 345, (9), (10)

$$(\psi_1 \psi_2 \cdots \psi_{\lambda-1}) f = S_{\lambda+1} \cdot f_\lambda - \varphi_{\lambda+1} S_\lambda \cdot f_{\lambda+1}, \tag{23}$$

$$(\psi_1 \psi_2 \cdots \psi_{\lambda-1}) f_1 = T_{\lambda+1} \cdot f_\lambda - \varphi_{\lambda+1} T_\lambda \cdot f_{\lambda+1}, \tag{24}$$

$$f T_\lambda - f_1 S_\lambda = -(\varphi_2 \varphi_3 \cdots \varphi_\lambda) f_\lambda, \tag{25}$$

$$f T_r - f_1 S_r = -\varphi_2 \varphi_3 \cdots \varphi_r. \tag{26}$$

Wir beweisen nun die folgenden Sätze: Die Function $S_{\lambda+1}$ ist durch das Product $d_1 d_2 \cdots d_{\lambda-1}$ theilbar. Wir nehmen an, der Satz wäre für S_λ und $d_1 d_2 \cdots d_{\lambda-2}$ schon bewiesen. Dann folgt aus (23)

$$\frac{\psi_1 \psi_2 \cdots \psi_{\lambda-1}}{d_1 d_2 \cdots d_{\lambda-1}} f = \frac{S_{\lambda+1}}{d_1 d_2 \cdots d_{\lambda-1}} f_\lambda - \frac{\varphi_{\lambda+1}}{d_{\lambda-1}} \frac{S_\lambda}{d_1 d_2 \cdots d_{\lambda-2}} f_{\lambda+1}, \tag{27}$$

hier ist nach der Definition der d_λ die linke Seite ganz; ebenso nach

Definition und nach der letzten Voraussetzung der zweite Summand der rechten Seite; also auch der erste. Da aber f_λ keinen von z_1 unabhängigen Theiler besitzt, so ist $S_{\lambda+1}$ durch $d_1 d_2 \cdots d_{\lambda-1}$ theilbar. Der Satz gilt daher allgemein, wenn er für $\lambda = 2$ richtig ist, wenn also S_3 durch $d_1 = 1$ sich theilen lässt. Das ist aber selbstverständlich.

Ebenso ist die Function $T_{\lambda+1}$ durch das Product $d_1 d_2 \cdots d_{\lambda-1}$ theilbar. Das folgt ebenso aus

$$(28)\qquad \frac{\psi_1 \psi_2 \cdots \psi_{\lambda-1}}{d_1\, d_2 \cdots d_{\lambda-1}} f_1 = \frac{T_{\lambda+1}}{d_1\, d_2 \cdots d_{\lambda-1}} f_\lambda - \frac{\varphi_{\lambda+1}}{d_{\lambda-1}} \frac{T_\lambda}{d_1\, d_2 \cdots d_{\lambda-2}} f_{\lambda+1}.$$

Wir können demnach aus (25) und (26) die Gleichungen folgern

$$(29)\qquad f \frac{T_\lambda}{d_1\, d_2 \cdots d_{\lambda-2}} - f_1 \frac{S_\lambda}{d_1\, d_2 \cdots d_{\lambda-2}} = -\left(\frac{\varphi_2}{1} \frac{\varphi_3}{d_1} \cdots \frac{\varphi_\lambda}{d_{\lambda-2}}\right) f_\lambda,$$

$$(30)\qquad f \frac{T_r}{d_1\, d_2 \cdots d_{r-2}} - f_1 \frac{S_r}{d_1\, d_2 \cdots d_{r-2}} = -\frac{\varphi_2}{1} \frac{\varphi_3}{d_1} \cdots \frac{\varphi_r}{d_{r-2}}.$$

Aus den vier letzten Gleichungen lassen sich die Labatie'schen Resultate ablesen. (30) zeigt, dass jede Wurzel (ζ_1, ζ_2) von (22) mindestens einen der Quotienten

$$(31)\qquad \frac{\varphi_2}{1},\ \frac{\varphi_3}{d_1},\ \frac{\varphi_4}{d_2},\ \cdots\ \frac{\varphi_r}{d_{r-2}},$$

welche sämmtlich ganze Functionen von z_2 allein sind, zum Verschwinden bringt. Es sei $\frac{\varphi_{\lambda+1}}{d_{\lambda-1}}$ die erste der Functionen (31), die für $z_2 = \zeta_2$ gleich 0 wird. Dann zeigt (29), dass $f_\lambda(\zeta_1, \zeta_2) = 0$ ist. Demnach wird für (ζ_1, ζ_2) sein müssen $f_\lambda = 0$, $\frac{\varphi_{\lambda+1}}{d_{\lambda-1}} = 0$.

Wenn umgekehrt (ζ_1, ζ_2) gleichzeitig die Functionen f_λ und $\frac{\varphi_{\lambda+1}}{d_{\lambda-1}}$ zu Null macht, dann zeigen (27) und (28), dass für (ζ_1, ζ_2) auch

$$\frac{\psi_1 \psi_2 \cdots \psi_{\lambda-1}}{d_1\, d_2 \cdots d_{\lambda-1}} \cdot f \quad \text{und} \quad \frac{\psi_1 \psi_2 \cdots \psi_{\lambda-1}}{d_1\, d_2 \cdots d_{\lambda-1}} \cdot f_1$$

verschwinden. Der erste Factor jedes dieser Producte ist relativ prim zu $\frac{\varphi_{\lambda+1}}{d_{\lambda-1}}$ und daher nicht gleich 0 für $z_2 = \zeta_2$. Deswegen wird $f(\zeta_1, \zeta_2) = 0$ und $f_1(\zeta_1, \zeta_2) = 0$. Somit gilt der Satz: Jede Wurzel von (22) befriedigt mindestens eins der Gleichungssysteme

$$(32)\qquad f_\lambda(z_1, z_2) = 0, \quad \frac{\varphi_{\lambda+1}(z_2)}{d_{\lambda-1}(z_2)} = 0 \qquad (\lambda = 1, 2, \cdots r-1);$$

und umgekehrt liefern die Wurzeln von (32) sämmtliche Wurzeln von (22).

Sechsunddreissigste Vorlesung.

Symmetrische Functionen mehrerer Grössenreihen.

§ 377. Wie bei zwei Gleichungen mit einer Unbekannten, so kann man auch bei drei Gleichungen mit zwei Unbekannten nach den charakteristischen Bedingungen für das Bestehen gemeinsamer Wurzeln fragen. Wenn

$$f(z_1, z_2) = 0, \quad g(z_1, z_2) = 0, \quad h(z_1, z_2) = 0$$

die drei Gleichungen sind, und $f = 0$, $g = 0$ eine endliche Anzahl von Wurzeln $\zeta_{11}, \zeta_{21}; \zeta_{12}, \zeta_{22}; \cdots \zeta_{1k}, \zeta_{2k}$ haben, dann besteht die gesuchte Bedingung offenbar darin, dass die „Resultante"

$$h(\zeta_{11}, \zeta_{21})\, h(\zeta_{12}, \zeta_{22}) \cdots h(\zeta_{1k}, \zeta_{2k}) = 0$$

sei. Diese Function links hat die Eigenthümlichkeit, dass sie sich nicht ändert, wenn man die zweiten Indices der ζ_1, ζ_2 beliebig unter einander vertauscht. Hierdurch kommt man zu dem Begriffe der symmetrischen Functionen von zwei Grössenreihen; und schon durch die soeben gegebenen Andeutungen wird ihre Bedeutung für die Theorie von Gleichungssystemen ersichtlich. Allgemein könnte man symmetrische Functionen von beliebig vielen Grössenreihen definiren und studiren; wir ziehen es aber vor, die Theorie für drei Reihen von je k Grössen

$$(1) \qquad (x_1, y_1, z_1), \quad (x_2, y_2, z_2), \quad \cdots \quad (x_k, y_k, z_k)$$

durchzuführen, da es hierbei schon völlig klar wird, wie die Resultate auf mehr Reihen zu übertragen sind, und da andererseits die Darstellung durch diese Beschränkung an Einfachheit gewinnt.

Wir nennen eine Function der unbestimmten Grössen (1) dann eine symmetrische Function dieser drei Reihen, wenn sie ihre Form bei jeder Vertauschung der unteren Indices $1, 2, \cdots k$ beibehält, oder, was das Gleiche aussagt, bei jeder Vertauschung der Tripel (1). Jede ganze Function dieser Eigenschaft heisst eine ganze symmetrische Function; jede ganze symmetrische Function, deren Glieder sämmtlich durch Vertauschung der Indices aus einem ihrer Glieder hergeleitet werden können, heisst eine eintypige symmetrische Function. Daraus folgt, dass jede ganze symmetrische Function als Summe von eintypigen symmetrischen Functionen dargestellt werden kann, so dass es ausreicht, statt allgemein ganze symmetrische Functionen zu betrachten, allein eintypige zu untersuchen.

So lange nur ein System von Grössen gegeben war, $z_1, z_2, \cdots z_k$, hatten wir als elementare symmetrische Functionen diejenigen hervorgehoben, welche von einer der Formen

$$S(z_1) = c_1, \quad S(z_1 z_2) = c_2, \quad \cdots \quad S(z_1 z_2 \cdots z_k) = c_k$$

waren, also diejenigen eintypigen, bei denen in jedem Summanden nur verschiedene untere Indices vorkommen. In ähnlicher Weise wollen wir hier **elementare symmetrische Functionen** der drei Reihen $x_\alpha, y_\alpha, z_\alpha$ diejenigen eintypigen nennen, in denen kein Summand den gleichen unteren Index mehrere Male besitzt. Die Bezeichnung geschieht am einfachsten mit Hülfe dieser Indices

$$(2) \quad \begin{aligned} &S(x_1) = c_{100}, \quad && S(y_1) = c_{010}, \quad && S(z_1) = c_{001}, \\ &S(x_1 x_2) = c_{200}, && S(y_1 y_2) = c_{020}, && S(z_1 z_2) = c_{002}, \\ &S(x_1 y_2) = c_{110}, && S(x_1 z_2) = c_{101}, && S(y_1 z_2) = c_{011}, \\ &S(x_1 \cdots x_\alpha y_{\alpha+1} \cdots y_{\alpha+\beta} z_{\alpha+\beta+1} \cdots z_{\alpha+\beta+\gamma}) = c_{\alpha\beta\gamma}. \end{aligned}$$

Dass unsere Definitionen für eine und für mehrere Reihen wirklich analoge Bildungen aufweisen, zeigt auch die folgende Betrachtung. Wir verstehen unter $\varkappa, \lambda, \mu$ willkürliche Parameter und bezeichnen

$$(3) \quad t_\alpha = \varkappa x_\alpha + \lambda y_\alpha + \mu z_\alpha \qquad (\alpha = 1, 2, \cdots k);$$

die symmetrischen Functionen der (3) nennen wir

$$(4) \quad S(t_1) = \gamma_1, \quad S(t_1 t_2) = \gamma_2, \quad S(t_1 t_2 t_3) = \gamma_3, \quad \cdots$$

und finden dann für sie

$$(5) \quad \begin{aligned} &\gamma_1 = \varkappa c_{100} + \lambda c_{010} + \mu c_{001}, \\ &\gamma_2 = \varkappa^2 c_{200} + \varkappa\lambda c_{110} + \varkappa\mu c_{101} + \lambda^2 c_{020} + \lambda\mu c_{011} + \mu^2 c_{002}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\gamma_\omega = \sum \varkappa^\varrho \lambda^\sigma \mu^\tau c_{\varrho\sigma\tau}, \qquad (\varrho + \sigma + \tau = \omega), \end{aligned}$$

so dass also die symmetrischen elementaren Functionen der Grössen (3) linear durch die der Reihen (1) dargestellt werden können.

Wir wollen weiter auch Functionen einführen, welche den **Potenzsummen** einer Reihe von Grössen $s_\alpha = S(z_1^\alpha)$ entsprechen. Diese s_α sind solche eintypige Functionen, bei denen nur ein einziger unterer Index in jedem Summanden auftritt. Dieselbe Definition behalten wir hier bei und setzen in entsprechender Weise

$$(6) \quad S(x_1^\alpha y_1^\beta z_1^\gamma) = s_{\alpha,\beta,\gamma}.$$

Bezeichnen wir die Potenzsummen der t_α mit $\sigma_1, \sigma_2, \sigma_3, \cdots$, so erkennen wir leicht, dass die σ sämmtlich linear aus den $s_{\alpha\beta\gamma}$ zusammengesetzt sind. Es wird nämlich

$$(7) \quad \begin{aligned} &\sigma_1 = \varkappa s_{100} + \lambda s_{010} + \mu s_{001}, \\ &\sigma_2 = \varkappa^2 s_{200} + 2\varkappa\lambda s_{110} + 2\varkappa\mu s_{101} + \lambda^2 s_{020} + 2\lambda\mu s_{011} + \mu^2 s_{002}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\sigma_\omega = \sum \frac{\omega!}{\varrho!\,\sigma!\,\tau!} \varkappa^\varrho \lambda^\sigma \mu^\tau s_{\varrho\sigma\tau}, \qquad (\varrho + \sigma + \tau = \omega). \end{aligned}$$

§ 378. Die in § 93, Bd. I aufgestellte Formel (7) liefert die Darstellungen der σ_α durch die γ_α. Trägt man in diese Formeln die Werthe (7) und (5) ein und setzt die Coefficienten gleicher Potenzproducte von $\varkappa$, λ, μ rechts und links einander gleich, so erhält man die $s_{\alpha\beta\gamma}$ sämmtlich durch die $c_{\alpha\beta\gamma}$ ausgedrückt. So erhält man beispielsweise die Resultate

$$
(8)\quad \begin{aligned}
&s_{100} = c_{100}, \quad s_{200} = c_{100}^2 - 2c_{200}, \quad s_{110} = c_{100}c_{010} - c_{110}, \cdots \\
&s_{300} = c_{100}^3 - 3c_{200}c_{100} + 3c_{300}, \; s_{210} = c_{100}^2 c_{010} - c_{200}c_{010} - c_{110}c_{100} + c_{210}, \\
&2s_{111} = 2c_{100}c_{010}c_{001} - c_{100}c_{011} - c_{010}c_{101} - c_{001}c_{110} + c_{111}, \cdots.
\end{aligned}
$$

Die letzte Formel zeigt, dass die s hierbei nicht nothwendig ganzzahlige ganze Functionen der c zu werden brauchen. (Vgl. § 385.)

Umgekehrt giebt die Formel (10) aus § 94 Bd. I die Darstellung der γ_α durch die σ_α und damit diejenige der $c_{\alpha\beta\gamma}$ durch die $s_{\alpha\beta\gamma}$. So erhält man z. B.

$$
(9)\quad \begin{aligned}
&c_{100} = s_{100}, \quad c_{010} = s_{010}, \cdots \\
&2c_{200} = s_{100}^2 - s_{200}, \quad c_{110} = s_{100}s_{010} - s_{110}, \cdots \\
&6c_{300} = s_{100}^3 - 3s_{100}s_{200} + 2s_{300}, \\
&2c_{210} = s_{100}^2 s_{010} - 2s_{100}s_{110} - s_{010}s_{200} + 2s_{210}, \\
&c_{111} = s_{100}s_{010}s_{001} - s_{100}s_{101} - s_{001}s_{101} - s_{001}s_{110} + 2s_{111}, \cdots
\end{aligned}
$$

Es ist nicht schwierig, mit Hülfe von (7), § 92 Bd. I und (10), § 94 Bd. I die zu (8) und (9) gehörigen allgemeinen Ausdrücke explicit darzustellen; doch hat das für uns keinen Zweck.

Ebenso können aus allen, früher für eine Variablenreihe aufgestellten Formeln durch Eintragung der γ und der σ neue hierher gehörige Beziehungen hergeleitet werden. So ergiebt z. B. die Formel

$$\sigma_{\alpha+k} - \gamma_1\sigma_{\alpha+k-1} + \gamma_2\sigma_{\alpha+k-2} - \cdots \pm \gamma_k\sigma_\alpha = 0$$

unter anderen die Recursionsformel

$$(\alpha+3)s_{\alpha+2,1,0} = (\alpha+2)c_{100}s_{\alpha+1,1,0} + c_{010}s_{\alpha+2,0,0} - c_{200}s_{\alpha,1,0} - c_{110}s_{\alpha+1,0,0}.$$

§ 379. Den Betrachtungen in § 96, Bd. I entsprechen jetzt ähnliche, mit deren Hülfe es gelingt, alle eintypigen Functionen durch die Potenzsummen $s_{\alpha\beta\gamma}$ und folglich nach dem vorigen Paragraphen auch durch die $c_{\alpha\beta\gamma}$ darzustellen.

Man hat zunächst, wenn $(\alpha_1 - \alpha_2)(\beta_1 - \beta_2)(\gamma_1 - \gamma_2) \neq 0$ ist, die Formel

$$S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1})\,S(x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2}) = S(x_1^{\alpha_1+\alpha_2}y_1^{\beta_1+\beta_2}z_1^{\gamma_1+\gamma_2}) + S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}\,x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2})$$

und also daraus

$$(10)\quad \begin{aligned} S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}\,x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2}) &= S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1})\,S(x_1^{\alpha_2}y_1^{\beta_2}z_1^{\gamma_2}) - S(x_1^{\alpha_1+\alpha_2}y_1^{\beta_1+\beta_2}z_1^{\gamma_1+\gamma_2}) \\ &= s_{\alpha_1\beta_1\gamma_1}s_{\alpha_2\beta_2\gamma_2} - s_{\alpha_1+\alpha_2,\,\beta_1+\beta_2,\,\gamma_1+\gamma_2}. \end{aligned}$$

Wenn alle Differenzen $\alpha_1-\alpha_2$, $\beta_1-\beta_2$, $\gamma_1-\gamma_2$ Null werden, dann und nur dann tritt in der vorletzten Formel eine Aenderung ein, indem der letzte Summand der rechten Seite in $2S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}x_2^{\alpha_1}y_2^{\beta_1}z_2^{\gamma_1})$ übergeht. Man hat deshalb als Ergänzungsformel

$$(10^a)\qquad S(x_1^{\alpha}y_1^{\beta}z_1^{\gamma}x_2^{\alpha}y_2^{\beta}z_2^{\gamma}) = \frac{1}{2}\left[s_{\alpha\beta\gamma}^2 - s_{2\alpha,2\beta,2\gamma}\right].$$

Mit Hülfe von (10) und (10ᵃ) kann man sonach sämmtliche eintypigen ganzen symmetrischen Functionen darstellen, in deren einzelne Glieder nicht mehr als zwei untere Indices eingehen. Die Methode für den weiteren Fortschritt ist jetzt ersichtlich.

Sind die drei Tripel $\alpha_1, \beta_1, \gamma_1$; $\alpha_2, \beta_2, \gamma_2$; $\alpha_3, \beta_3, \gamma_3$ von einander verschieden, d. h. so beschaffen, dass nicht gleichzeitig die drei Elemente des einen gleich den drei entsprechenden eines anderen sind, dann ergiebt sich

$$\begin{aligned} S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2})\,S(x_1^{\alpha_3}y_1^{\beta_3}z_1^{\gamma_3}) &= S(x_1^{\alpha_1+\alpha_3}y_1^{\beta_1+\beta_3}z_1^{\gamma_1+\gamma_3}x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2}) \\ &+ S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}x_2^{\alpha_2+\alpha_3}y_2^{\beta_2+\beta_3}z_2^{\gamma_2+\gamma_3}) + S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2}x_3^{\alpha_3}y_3^{\beta_3}z_3^{\gamma_3}) \end{aligned}$$

und also daraus mit Hülfe von (10)

$$(11)\quad \begin{aligned} S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}x_2^{\alpha_2}y_2^{\beta_2}z_2^{\gamma_2}x_3^{\alpha_3}y_3^{\beta_3}z_3^{\gamma_3}) &= s_{\alpha_1\beta_1\gamma_1}s_{\alpha_2\beta_2\gamma_2}s_{\alpha_3\beta_3\gamma_3} - s_{\alpha_1\beta_1\gamma_1}s_{\alpha_2+\alpha_3,\beta_2+\beta_3,\gamma_2+\gamma_3} \\ &- s_{\alpha_2\beta_2\gamma_2}s_{\alpha_1+\alpha_3,\beta_1+\beta_3,\gamma_1+\gamma_3} - s_{\alpha_3\beta_3\gamma_3}s_{\alpha_1+\alpha_2,\beta_1+\beta_2,\gamma_1+\gamma_2} + 2s_{\alpha_1+\alpha_2+\alpha_3,\beta_1+\beta_2+\beta_3,\gamma_1+\gamma_2+\gamma_3}. \end{aligned}$$

Auch hierzu gehören ergänzende Formeln. Ist etwa $\alpha_1=\alpha_2$, $\beta_1=\beta_2$, $\gamma_1=\gamma_2$, aber $\alpha_3, \beta_3, \gamma_3$ von $\alpha_1, \beta_1, \gamma_1$ verschieden, so wird jedes Glied von $S(x_1^{\alpha_1}y_1^{\beta_1}z_1^{\gamma_1}x_2^{\alpha_1}y_2^{\beta_1}z_2^{\gamma_1}x_3^{\alpha_3}y_3^{\beta_3}z_3^{\gamma_3})$ links in (11) zweimal auftreten. Demnach entsteht

$$(11^a)\quad \begin{aligned} S(x_1^{\alpha}y_1^{\beta}z_1^{\gamma}x_2^{\alpha}y_2^{\beta}z_2^{\gamma}x_3^{\alpha_1}y_3^{\beta_1}z_3^{\gamma_1}) &= \frac{1}{2}s_{\alpha\beta\gamma}^2 s_{\alpha_1\beta_1\gamma_1} - s_{\alpha\beta\gamma}s_{\alpha+\alpha_1,\beta+\beta_1,\gamma+\gamma_1} \\ &- \frac{1}{2}s_{\alpha_1\beta_1\gamma_1}s_{2\alpha,2\beta,2\gamma} + s_{2\alpha+\alpha_1,2\beta+\beta_1,2\gamma+\gamma_1}. \end{aligned}$$

Wenn endlich auch noch $\alpha_1=\alpha_2=\alpha_3$, $\beta_1=\beta_2=\beta_3$, $\gamma_1=\gamma_2=\gamma_3$ wird, wiederholt sich links in (11) jedes Glied sechsmal. Deshalb muss gesetzt werden

$$(11^b)\quad S(x_1^{\alpha}y_1^{\beta}z_1^{\gamma}x_2^{\alpha}y_2^{\beta}z_2^{\gamma}x_3^{\alpha}y_3^{\beta}z_3^{\gamma}) = \frac{1}{6}s_{\alpha\beta\gamma}^3 - \frac{1}{2}s_{\alpha\beta\gamma}s_{2\alpha,2\beta,2\gamma} + \frac{1}{3}s_{3\alpha,3\beta,3\gamma}.$$

Da man genau in derselben Weise die Berechnung symmetrischer eintypiger Functionen mit $(\nu+1)$ unteren Indices auf solche mit ν Indices zurückführen kann, so folgt der bereits angekündigte Satz: Jede symmetrische ganze Function ist als ganze Function der $s_{\alpha\beta\gamma}$ und folglich auch der $c_{\alpha\beta\gamma}$ darstellbar*).

*) Poisson, Journ. d. l'École Polyt. XI cah. p. 199 (An X)

§ 380. Die im vorigen Paragraphen gewonnene Methode der Darstellung symmetrischer Functionen durch die elementaren ist indirect und zudem bei der Ausführung recht mühsam. Man könnte versuchen, eine der früher bei einer Elementenreihe besprochenen (§ 97 und § 102, Bd. I) auf mehrere Variablenreihen auszudehnen. Aber beide, die Gauss'sche sowohl wie die Cauchy'sche versagen, wie man leicht erkennt.

Zur wirklichen, praktischen Benutzung empfiehlt sich die Anwendung unbestimmter Coefficienten. Sie ist, nachdem man den litteralen Theil der Aufgabe gelöst hat, verhältnissmässig bequem durchzuführen.

Für die Herstellung des litteralen Theils gelten folgende Regeln. Ist etwa

$$(12)\qquad S(x_1^{\alpha_1} y_1^{\beta_1} z_1^{\gamma} \cdots x_3^{\alpha_3} y_3^{\beta_3} z_3^{\gamma_3}) = \sum k_{a_1 b_1 c_1, a_2 b_2 c_2, \ldots} c_{a_1 b_1 c_1} c_{a_2 b_2 c_2} \cdots$$

zu behandeln, wobei die c die elementaren symmetrischen Functionen und die k unbekannte Zahlencoefficienten bedeuten, dann braucht man nur solche aus den c gebildeten Producte zu betrachten, für welche

$$(13)\qquad \begin{aligned} a_1 + a_2 + \cdots &= \alpha_1 + \alpha_2 + \alpha_3, \\ b_1 + b_2 + \cdots &= \beta_1 + \beta_2 + \beta_3, \\ c_1 + c_2 + \cdots &= \gamma_1 + \gamma_2 + \gamma_3 \end{aligned}$$

wird. Denn setzt man statt der $x_1, x_2, \cdots x_k$ etwa $x_1 t, x_2 t, \cdots x_k t$, dann tritt in (12) aus der linken Seite $t^{\alpha_1+\alpha_2+\alpha_3}$ heraus; rechts geht jedes $c_{a_1 b_1 c_1}$ in ein $t^{a_1} c_{a_1 b_1 c_1}$ über, so dass also $a_1 + a_2 + \cdots = \alpha_1 + \alpha_2 + \alpha_3$ sein muss, wie die erste der drei Gleichungen (13) behauptet. Aehnlich erkennt man die Richtigkeit der beiden folgenden Gleichungen (13). Durch diese Regel wird die Anzahl der überhaupt möglichen Glieder der rechten Seite in (12) stark beschränkt.

Die Summe sämmtlicher Exponenten

$$\sum \alpha + \sum \beta + \sum \gamma$$

nennen wir das Gesammtgewicht der symmetrischen Functionen S (vgl. § 99 Bd. I). $\sum \alpha$ heisst das Partialgewicht von S nach den x, u. s. w. Eine eintypige Function ist isobarisch im Gesammtgewichte und in den Partialgewichten. (13) zeigt, dass jeder Summand rechts in (12) im Gewichte mit dem eintypigen S der linken Seite übereinstimmt.

Die Gesammtzahl der Factoren c rechts in (12) kann die Höhe des Gesammtgewichtes nicht überschreiten, da jedes c mindestens eine Einheit zum Gesammtgewichte beisteuert. Dieses Maximum der Factorenanzahl wird bei gewissen Functionen, z. B. bei den $s_{\alpha\beta\gamma}$ auch

wirklich erreicht, wie (8) zeigt, und wie sich allgemein gleichfalls leicht nachweisen lässt, sobald man auf die Darstellung der σ durch die γ zurückgeht.

Wir wollen das Besprochene an einem Beispiele darlegen. Ist

$$a_1 + a_2 + \cdots = 2, \quad b_1 + b_2 + \cdots = 2, \quad c_1 + c_2 + \cdots = 0,$$

so wird in den $c_{\alpha\beta\gamma}$ der dritte Index stets Null sein, und es können nicht mehr als vier Factoren in jedem Summanden vorkommen. Es sind deswegen nur folgende neun Glieder möglich:

$$k_1 c_{100}^2 c_{010}^2, \quad k_2 c_{100}^2 c_{020}, \quad k_3 c_{100} c_{010} c_{110}, \quad k_4 c_{010}^2 c_{200}, \quad k_5 c_{100} c_{120},$$
$$k_6 c_{010} c_{210}, \quad k_7 c_{110}^2, \quad k_8 c_{200} c_{020}, \quad k_9 c_{220}.$$

Dies findet statt, wie auch immer die Zahlen 2 in Summen $a_1 + a_2 + \cdots$ oder $b_1 + b_2 + \cdots$ zerlegt werden mögen.

§ 381. Zu der Bestimmung der Coefficienten k kann man auf zweierlei Art gelangen. Zunächst so, dass man eine Reihe von speciellen Zahlenwerthen für die x, y, z nimmt, daraus den Werth der symmetrischen, darzustellenden Function, sowie die $c_{\alpha\beta\gamma}$ berechnet, Alles dies in (12) einträgt und dadurch zu einer linearen Gleichung für die unbekannten Grössen k gelangt. Hat man hinreichend viele solcher linearen Gleichungen aufgestellt, so folgen aus ihrer Auflösung die Werthe der k.

Wir wollen diese Vorschriften bei der Berechnung der Function $S(x_1^2 y_2 y_3)$ durchführen, wobei also wegen $a_1 + a_2 = 2$, $b_1 + b_2 = 2$, $c_1 + c_2 = 0$ die oben aufgestellten Summanden die einzig möglichen sind. Wir müssen deswegen neun besondere Annahmen machen. Die z können wir stets bei Seite lassen.

I. $x_1 = 1, \; y_1 = 1; \;\; x_2 = 0, \; y_2 = 0; \;\; x_3 = 0, \; y_3 = 0, \cdots; \;\; S = 0;$
$c_{100} = 1, \;\; c_{010} = 1, \;\; c_{200} = 0, \cdots;$

Resultat: $k_1 = 0$.

II. $x_1 = 1, \; y_1 = 1; \;\; x_2 = 1, \; y_2 = 0; \;\; x_3 = 0, \; y_3 = 0, \cdots; \;\; S = 0;$
$c_{100} = 2, \;\; c_{010} = 1, \;\; c_{110} = 1, \;\; c_{020} = 0, \cdots;$
$2k_3 + k_4 + k_7 = 0.$

III. $x_1 = 1, \; y_1 = 1; \;\; x_2 = 0, \; y_2 = 1; \;\; x_3 = 0, \; y_3 = 0; \cdots; \;\; S = 0;$
$c_{100} = 1, \;\; c_{010} = 2, \;\; c_{200} = 0, \;\; c_{110} = 1, \;\; c_{020} = 1, \;\; c_{300} = 0, \cdots;$
$k_2 + 2k_3 + k_7 = 0.$

IV. $x_1 = 1, \; y_1 = 1; \;\; x_2 = 2, \; y_2 = 0; \;\; x_3 = 0, \; y_3 = 0; \cdots; \;\; S = 0;$
$c_{100} = 3, \;\; c_{010} = 1, \;\; c_{200} = 2, \;\; c_{110} = 2, \;\; c_{020} = 0, \cdots;$
$3k_3 + k_4 + 2k_7 = 0.$

Die drei letzten Gleichungen liefern die Beziehungen

$$k_3 = -k_2, \quad k_4 = k_2, \quad k_7 = k_2.$$

V. $x_1 = 1,\ y_1 = 1;\ x_2 = 1,\ y_2 = 1;\ x_3 = 0,\ y_3 = 0, \cdots;\ S = 0;$
$c_{100} = 2,\ c_{010} = 2,\ c_{200} = 1,\ c_{110} = 2,\ c_{020} = 1,\ c_{300} = 0, \cdots;$
$k_8 = -4k_2.$

VI. $x_1 = 1,\ y_1 = 1;\ x_2 = 1,\ y_2 = 0;\ x_3 = 1,\ y_3 = 0, \cdots;\ S = 0;$
$c_{100} = 3,\ c_{010} = 1,\ c_{200} = 3,\ c_{110} = 2,\ c_{020} = 0,\ c_{210} = 1,\ c_{120} = 0, \cdots;$
$k_6 = -k_2.$

VII. $x_1 = 1;\ y_1 = 1;\ x_2 = 0,\ y_2 = 1;\ x_3 = 0,\ y_3 = 1, \cdots;\ S = 1;$
$c_{100} = 1,\ c_{010} = 3,\ c_{200} = 0,\ c_{110} = 2,\ c_{020} = 3,\ c_{210} = 0,\ c_{120} = 1, \cdots$
$k_5 = 1 - k_2.$

VIII. $x_1 = 1,\ y_1 = 1;\ x_2 = 1,\ y_2 = 1;\ x_3 = 1,\ y_3 = 1, \cdots;\ S = 3;$
$c_{100} = 3,\ c_{010} = 3,\ c_{200} = 3,\ c_{110} = 6,\ c_{020} = 3,\ c_{210} = 3,\ c_{120} = 3, \cdots$
$k_8 = -\frac{2}{3} - 2k_2.$

Die bisherigen Resultate liefern nunmehr insgesammt

$$k_2 = \frac{1}{3},\ k_3 = -\frac{1}{3},\ k_4 = \frac{1}{3},\ k_5 = \frac{2}{3},\ k_6 = -\frac{1}{3},\ k_7 = \frac{1}{3},\ k_8 = -\frac{4}{3}.$$

IX. $x_1 = x_2 = x_3 = x_4 = 1;\ y_1 = y_2 = y_3 = y_4 = 1;\ x_5 = y_5 = \cdots = 0;\ S = 12;$
$c_{100} = 4,\ c_{010} = 4,\ c_{200} = 6,\ c_{110} = 12,\ c_{020} = 6,\ c_{210} = 12,\ c_{200} = 6;\ c_{220} = 6;$
$k_9 = -\frac{2}{3}.$

Damit haben wir also erlangt, wenn wir die dritten Indices unterdrücken,

$$(14) \qquad S(x_1^2 y_2 y_3) = \frac{1}{3}\Big\{c_{10}^2 c_{02} - c_{10} c_{01} c_{11} + c_{01}^2 c_{20} + 2 c_{10} c_{12} - c_{01} c_{21} + c_{11}^2 - 4 c_{20} c_{02} - 2 c_{22}\Big\}.$$

§ 382. Die Berechnung der k kann ferner auch derart stattfinden, dass man jedes Product der c auf der rechten Seite von (12) durch die x, y, z ausdrückt, dann die gleichen symmetrischen Functionen der Elemente, welche rechts in den einzelnen Summanden auftreten, sammelt und durch passende Wahl der k alle diejenigen zum Verschwinden bringt, welche links nicht vorkommen.

Im Falle

$$a_1 + a_2 + \cdots = 2, \quad b_1 + b_2 + \cdots = 2, \quad c_1 + c_2 + \cdots = 0$$

würde sich die Rechnung folgendermassen gestalten. Es ist

$$c_{100}^2 c_{010}^2 = Sx_1^2 y_1^2 + 2Sx_1^2 y_1 y_2 + 2Sx_1^2 y_2 y_3 + Sx_1^2 y_2^2 + 2Sx_1 x_2 y_1^2$$
$$+ 4Sx_1 x_2 y_1 y_2 + 4Sx_1 x_2 y_1 y_3 + 2Sx_1 x_2 y_3^2 + 4Sx_1 x_2 y_3 y_4,$$
$$c_{100}^2 c_{020} = Sx_1^2 y_1 y_2 + Sx_1^2 y_2 y_3 + 2Sx_1 x_2 y_1 y_2 + 2Sx_1 x_2 y_1 y_3 + 2Sx_1 x_2 y_3 y_4,$$
$$c_{100} c_{010} c_{110} = Sx_1^2 y_1 y_2 + Sx_1^2 y_2^2 + 2Sx_1^2 y_2 y_3 + Sx_1 x_2 y_1^2 + 2Sx_1 x_2 y_1 y_2$$
$$+ 3Sx_1 x_2 y_1 y_3 + 2Sx_1 x_2 y_3^2 + 4Sx_1 x_2 y_3 y_4,$$
$$c_{010}^2 c_{200} = Sx_1 x_2 y_1^2 + 2Sx_1 x_2 y_1 y_2 + 2Sx_1 x_2 y_1 y_3 + Sx_1 x_2 y_3^2 + 2Sx_1 x_2 y_3 y_4,$$
$$c_{100} c_{120} = Sx_1^2 y_2 y_3 + Sx_1 x_2 y_1 y_3 + 2Sx_1 x_2 y_3 y_4,$$
$$c_{010} c_{210} = Sx_1 x_2 y_1 y_3 + 2Sx_1 x_2 y_3 y_4 + Sx_1 x_2 y_3^2,$$
$$c_{110}^2 = Sx_1^2 y_2^2 + 2Sx_1^2 y_2 y_3 + 2Sx_1 x_2 y_1 y_2 + 2Sx_1 x_2 y_1 y_3 + 2Sx_1 x_2 y_3^2$$
$$+ 4Sx_1 x_2 y_3 y_4,$$
$$c_{200} c_{020} = Sx_1 x_2 y_1 y_2 + Sx_1 x_2 y_1 y_3 + Sx_1 x_2 y_3 y_4,$$
$$c_{220} = Sx_1 x_2 y_3 y_4.$$

Es ist daher jede ganze symmetrische eintypige Function

$$S(x_1^{\alpha_1} y_1^{\beta_1} x_2^{\alpha_2} y_2^{\beta_2}) \qquad (\alpha_1 + \alpha_2 = \beta_1 + \beta_2 = 2) \tag{15}$$

in der folgenden Form darstellbar

$$\begin{aligned} & k_1 Sx_1^2 y_1^2 + (2k_1 + k_2 + k_3) S(x_1^2 y_1 y_2) + (k_1 + k_3 + k_7) S(x_1^2 y_2^2) \\ & + (2k_1 + k_2 + 2k_3 + k_5 + 2k_7) S(x_1^2 y_2 y_3) + (2k_1 + k_3 + k_4) S(x_1 x_2 y_1^2) \\ & + (4k_1 + 2k_2 + 2k_3 + 2k_4 + 2k_7 + k_8) S(x_1 x_2 y_1 y_2) \\ & + (4k_1 + 2k_2 + 3k_3 + 2k_4 + k_5 + k_6 + 2k_7 + k_8) S(x_1 x_2 y_1 y_3) \\ & + (2k_1 + 2k_3 + k_4 + k_6 + 2k_7) S(x_1 x_2 y_3^2) \\ & + (4k_1 + 2k_2 + 4k_3 + 2k_4 + 2k_5 + 2k_6 + 4k_7 + k_8 + k_9) S(x_1 x_2 y_3 y_4). \end{aligned} \tag{16}$$

Setzt man nun z. B. den Coefficienten von $Sx_1^2 y_2 y_3$ gleich 1 und alle übrigen Coefficienten in (16) gleich Null, dann erhält man wieder das Resultat (14). Man erkennt, dass, wenn einmal die Formel (16) abgeleitet ist, die unter (15) fallenden Functionen sämmtlich ohne besondere Mühe hergestellt werden können.

Der in § 379 gelieferte Beweis für die Existenz einer solchen Darstellung jedes S durch die c bietet die Gewähr dafür, dass beide Methoden der Bestimmung der k wirklich zum Ziele führen, dass also die erlangten linearen Gleichungen keine Widersprüche bergen*). Da-

---

*) Ueber den behandelten Gegenstand vgl. Schläfli, „Ueber die Resultante eines Systems mehrerer algebraischen Gleichungen", Wiener Denkschriften IV (1852). — Cayley, „On the symmetric functions of the roots of certain systems of two equations". Phil. Trans. Vol. 147 (1837). — Mac-Mahon, „Memoir on symmetric functions of the roots of systems of equations". Phil. Trans. Vol. 181 (1890).

gegen wissen wir nicht, ob auf diesem Wege eine eindeutige Bestimmung der k möglich ist. Mit dieser Frage kommen wir zur Darlegung eines wesentlichen Unterschiedes, der zwischen den elementaren symmetrischen Functionen einer und denjenigen mehrerer Reihen von Variablen besteht.

§ 383. Es giebt, wie man leicht erkennt, bei r Reihen $x_\alpha, y_\alpha, \cdots u_\alpha$ $(\alpha = 1, 2, \cdots k)$ von je k Grössen r elementare symmetrische Functionen der Dimension 1, nämlich $\sum x_\alpha$, $\sum y_\alpha, \cdots \sum u_\alpha$; ferner $\frac{(r+1)r}{1 \cdot 2}$ solche von der Dimension 2, nämlich $\sum x_\alpha^2, \sum x_\alpha, y_\alpha, \cdots$ u. s. f. bis zu solchen von der Dimension k, zusammen also

$$\binom{r}{1} + \binom{r+1}{2} + \binom{r+2}{3} + \cdots + \binom{r+k-1}{k} = \left[\binom{r+1}{1} - \binom{r}{0}\right] + \left[\binom{r+2}{2} - \binom{r+1}{1}\right] + \cdots = \binom{r+k}{k} - 1.$$

Zwischen diesen elementaren symmetrischen Functionen besteht eine grosse Anzahl rationaler Gleichungen. Die Bildung eines Systems, welches nur unabhängige Functionen enthält, durch deren Hülfe alle anderen Functionen sich rational darstellen lassen, geschieht wohl am einfachsten auf dem folgenden Wege. Wir beschränken uns dabei wieder auf den Fall $r = 3$.

Man hat das System der k linearen Gleichungen für die x

$$(17) \quad \begin{array}{llll} x_1 & + x_2 & + \cdots = c_{100}, \\ x_1(c_{001} - z_1) & + x_2(c_{001} - z_2) & + \cdots = c_{101}, \\ x_1(c_{002} - c_{001}z_1 + z_1^2) & + x_2(c_{002} - c_{001}z_2 + z_2^2) & + \cdots = c_{102}, \\ \cdots & \cdots & \cdots \end{array}$$

dessen Auflösung, wie man mit Hülfe von § 88, Bd. I erkennt,

$$(18) \quad x_\alpha = \frac{c_{100} z_\alpha^{k-1} - c_{101} z_\alpha^{k-2} + c_{102} z_\alpha^{k-3} - \cdots}{k z_\alpha^{k-1} - (k-1) c_{001} z_\alpha^{k-2} + (k-2) c_{002} z_\alpha^{k-3} - \cdots} \quad (\alpha = 1, 2, \cdots k)$$

ergiebt. Ebenso erhält man für die y

$$(19) \quad y_\alpha = \frac{c_{010} z_\alpha^{k-1} - c_{011} z_\alpha^{k-2} + e_{012} c_\alpha^{k-3} - \cdots}{k z_\alpha^{k-1} - (k-1) c_{001} z_\alpha^{k-2} + (k-2) c_{002} z_\alpha^{k-3} - \cdots} \quad (\alpha = 1, 2, \cdots k).$$

Die Bedeutung der im Nenner auftretenden Function ist klar. Man hat für ein unbestimmtes ζ die Gleichung

$$\varphi(\zeta) = (\zeta - z_1)(\zeta - z_2) \cdots (\zeta - z_k) = \zeta^k - c_{001} \zeta^{k-1} + c_{002} \zeta^{k-2} - \cdots,$$

so dass

$$k z_\alpha^{k-1} - (k-1) c_{001} z_\alpha^{k-2} + (k-2) c_{002} z_\alpha^{k-3} - \cdots = \varphi'(z_\alpha)$$

ist. Daraus ersieht man, dass zu jedem System $c_{001}, c_{002}, \cdots c_{00,k-1}$ die k Grössen $z_1, z_2, \cdots z_k$ gefunden werden können, ja sogar, da c_{00k} nicht zu diesen c gehört, auf unendlich viele Arten; und dass dann, sobald diese z_α von einander verschieden, die Nenner in (18) und (19) also nicht Null sind, für jedes System $c_{100}, c_{101}, \cdots c_{10\alpha}, \cdots; c_{010}, c_{011}, \cdots c_{01\alpha}, \cdots$ eindeutig ein System x_α, y_α sich den z_α zuordnet. Es sind demnach die Grössen

$$(20)\qquad c_{001}, c_{002}, \cdots c_{0,0,k-1};\; c_{100}, c_{101}, \cdots c_{1,0,k-1};\; c_{010}, c_{011}, \cdots c_{0,1,k-1}$$

von einander unabhängige elementare symmetrische Functionen.

In (18) und (19) sind nur diese $(3k-1)$ Grössen (20) benutzt. Von den übrigen Grössen c enthält nur c_{00k} kein x und kein y. Die übrigen noch vorhandenen, deren Zahl

$$\binom{r+k}{k} - 1 - 3k$$

beträgt, wollen wir generell mit $c_{\varrho\sigma\tau}$ bezeichnen. Drückt man ein solches $c_{\varrho\sigma\tau}$ durch die Elemente x, y, z aus und ersetzt die in jeden Summanden eingehenden x_α, y_α durch ihre Werthe (18) und (19), so erhält man eine symmetrische gebrochene Function der z_α. Diese ist durch die $c_{001}, \cdots c_{00k}$ rational ausdrückbar, und so haben wir jedes der $c_{\varrho\sigma\tau}$ durch die $3k$ Grössen

$$(20^a)\qquad c_{001}, c_{002}, \cdots c_{00k};\; c_{100}, c_{101}, \cdots c_{10,k-1};\; c_{010}, c_{011}, \cdots c_{01,k-1}$$

dargestellt. In den Nenner tritt dabei, weil z. B. $(x_1 \cdots x_\varrho y_{\varrho+1} \cdots y_{\varrho+\sigma} z_{\varrho+\sigma+1} \cdots z_{\varrho+\sigma+\tau})$ durch

$$\varphi'(z_1) \cdots \varphi'(z_\varrho)\varphi'(z_{\varrho+1}) \cdots \varphi'(z_{\varrho+\sigma})$$

zu dividiren ist, einfach $\varphi'(z_1) \cdots \varphi'(z_k)$, d. h. die Discriminante D_φ von $\varphi(z)$ oder ein Theiler von ihr. Sonach ergiebt sich

$$(21)\qquad D_\varphi \cdot c_{\varrho\sigma\tau} = F_{\varrho\sigma\tau}(c_{00\alpha}, c_{10\beta}, c_{01\gamma}).$$

Giebt man jedem der c ein Gewicht, welches gleich der Summe seiner Indices ist, oder, was damit übereinstimmt, giebt man jedem x, y, z das Gewicht 1, dann wird (21) eine isobarische Beziehung vom Gewichte $k(k-1) + \varrho + \sigma + \tau$.

Ist z. B. $k = 2$, so gehen (18) und (19) in

$$x_1 = \frac{c_{100} z_1 - c_{101}}{2 z_1 - c_{001}}, \quad y_1 = \frac{c_{010} z_1 - c_{011}}{2 z_1 - c_{001}},$$

$$x_2 = \frac{c_{100} z_2 - c_{101}}{2 z_2 - c_{001}}, \quad y_2 = \frac{c_{010} z_2 - c_{011}}{2 z_2 - c_{001}}$$

über; die $\binom{5}{2} - 1 - 6 = 3$ Relationen heissen dann

$$c_{200}(4c_{002} - c_{001}^2) = c_{100}^2 c_{002} - c_{100} c_{101} c_{001} + c_{101}^2;$$
$$c_{110}(4c_{002} - c_{001}^2) = 2c_{100} c_{010} c_{002} - c_{101\,010} c_{001} - c_{100} c_{011} c_{001} + 2c_{101} c_{011};$$
$$c_{020}(4c_{002} - c_{001}^2) = c_{010}^2 c_{002} - c_{010} c_{011} c_{001} + c_{011}^2.$$

So erkennt man: Im allgemeinen Falle bilden die Functionen $c_{\alpha_1, \alpha_2 \cdots \alpha_r}$, für welche

$$\alpha_1 = \cdots = \alpha_{r-1} = 0; \quad \alpha_r = 1, 2, \cdots k$$

nebst denjenigen, für welche

$$\alpha_1 = \cdots = \alpha_{i-1} = \alpha_{i+1} = \cdots = \alpha_{r-1} = 0; \; \alpha_i = 1; \; \alpha_r = 0, 1, \cdots k-1; \; i = 1, 2, \cdots r-1$$

ist, ein unabhängiges System. Durch die Darstellung der übrigen c vermittels der angegebenen $c_{\alpha_1 \cdots \alpha_r}$ entstehen

$$\binom{k+r}{r} - kr - 1$$

rationale Relationen unter den elementaren symmetrischen Functionen. Diese sind von einander unabhängig, und alle überhaupt vorhandenen Relationen sind durch sie rational darstellbar.

Der Inhalt des letzten Satzes ist noch zu begründen. Die Unabhängigkeit der Relationen folgt einfach daraus, dass in jeder eins der neuen c linear auftritt und nur in dieser einen Relation vorkommt.

Wäre ferner irgend eine Relation zwischen den $c_{\alpha\beta\gamma}$ gegeben — wir kehren zum Falle $r = 3$ zurück —, so könnten durch (21) alle darin auftretenden $c_{\varrho\sigma\tau}$ eliminirt werden; dadurch erhielten wir eine Relation zwischen den Grössen (20[a]), welche doch von einander unabhängig sind. Folglich muss die Elimination auf eine identisch erfüllte Gleichung führen*).

§ 384. Das im vorigen Paragraphen hergeleitete System von Relationen zwischen den c zeichnet sich durch seine Uebersichtlichkeit, sowie dadurch aus, dass die Unabhängigkeit der einzelnen aufgestellten Gleichungen unter einander selbstverständlich ist. Dagegen sind die Relationen, nach der Höhe ihrer Gewichte betrachtet, nicht die einfachsten, welche es giebt, und es lassen sich noch andere Bildungsmethoden für Relationen angeben, bei denen niedrigere Gewichte erlangt werden.

So erhält man aus (18) und (19)

$$x_\alpha(c_{010} z_\alpha^{k-1} - c_{011} z_\alpha^{k-2} + \cdots) = y_\alpha(c_{100} z_\alpha^{k-1} - c_{101} z_\alpha^{k-2} + \cdots).$$

---

*) Eingehende Untersuchungen über diese Relationen, ihre Herstellung und ihre Minimalgewichte hat Herr Fr. Junker angestellt, Math. Ann. 38 (1891), p. 92 und ibid. 43 (1893), p. 225.

Erhebt man diese Gleichung in die λ^{te} Potenz und summirt nach α, dann entsteht

$$\overset{\lambda}{c}_{010}\, s_{\lambda,0,(k-1)\lambda} - \lambda \overset{\lambda-1}{c}_{010}\, c_{011} s_{\lambda,0,(k-1)\lambda-1} + \cdots = \overset{\lambda}{c}_{100}\, s_{0,\lambda,(k-1)\lambda} - \cdots;$$

für $\lambda = 2$ wird das Gewicht dieser Relation $(2k+2)$. Ebenso könnte man die vorletzte Gleichung mit $x_\alpha^{\varrho-1} y_\alpha^\sigma z_\alpha^{\tau-k+1}$ multipliciren und nach α summiren, dann entstände

$$c_{010} s_{\varrho,\sigma,\tau} - c_{011} s_{\varrho,\sigma,\tau-1} + \cdots = c_{100} s_{\varrho-1,\sigma+1,\tau} - c_{101} s_{\varrho-1,\sigma+1,\tau-1} + \cdots$$

vom Gewichte $\varrho + \sigma + \tau + 1$; u. s. f. Aber hierbei ist es fraglich, ob nicht, nachdem die s durch die c ersetzt sind (nach (8)), alle Glieder links und rechts sich zerstören. Es wäre also vor allem zu untersuchen, welches das Minimalgewicht einer nicht verschwindenden Relation ist. Herr Junker hat l. c. für die untere Grenze den Werth $(k+2)$ gefunden. Wir wollen auf diese Untersuchungen hier aber nicht eingehen.

§ 385. Die Herleitung unserer Relationen knüpft die Gültigkeit an das zu Grunde gelegte k. So ist z. B. (vgl. S. 73 Z. 1)

$$c_{100}^2 c_{002} - c_{100} c_{101} c_{001} + c_{101}^2 + c_{200}(c_{001}^2 - 4c_{002})$$

für $k = 2$ gleich Null. Für $k = 3$ hat dieser Ausdruck dagegen den Wert

$$Sx_1^2 z_2 z_3 + Sx_1 x_2 z_3^2 - Sx_1 x_2 z_2 z_3.$$

Es fragt sich aber noch, ob es nicht auch Relationen giebt, welche für unbestimmte k, d. h. für jeden Werth von k gültig sind. Wir werden zeigen, dass dies nicht der Fall ist.

Gesetzt, wir fügen zu unseren k Tripeln (1) noch ein Tripel (ξ, η, ζ) hinzu und bezeichnen die neuen elementaren symmetrischen Functionen mit $\gamma_{\lambda\mu\nu}$, dann folgt sofort

$$\gamma_{\lambda\mu\nu} = c_{\lambda\mu\nu} + \xi c_{\lambda-1,\mu,\nu} + \eta c_{\lambda,\mu-1,\nu} + \zeta c_{\lambda,\mu,\nu-1},$$

und diese Relation bleibt auch für einen Index 1 oder 0 richtig, falls $c_{000} = 1$ und ein c mit negativem Index gleich Null gesetzt wird.

Wir nehmen nun an, es sei bereits in einfachster Form

$$H(c_{\lambda\mu\nu}) = 0$$

eine Relation, welche für jedes k gültig bleibt, und welche zugleich unter allen etwa existirenden das Minimalgewicht besitzt. Dann müsste auch

$$H(\gamma_{\lambda\mu\nu}) = H(c_{\lambda\mu\nu} + \xi c_{\lambda-1,\mu,\nu} + \cdots) = 0$$

sein, und da ξ, η, ζ beliebige Grössen sind, müssten die Coefficienten aller Potenzproducte von ξ, η, ζ verschwinden. Wir betrachten den

Coefficienten der höchsten vorkommenden Potenz von ξ. Dieser entsteht aus denjenigen Gliedern von H, welche möglichst viele $c_{\lambda\mu\nu}$ (mit $\lambda > 0$) als Factoren besitzt, und er kann nicht für willkürliche c verschwinden, weil das Gleiche sonst auch bei jenen Gliedern von H stattfinden würde, die man hätte tilgen können. Dieser Coefficient hat ein geringeres Gesammtgewicht als H; das verstösst gegen die über H gemachte Voraussetzung hinsichtlich des Minimalgewichtes. Folglich besteht eine solche Relation nicht.

Bei unbestimmten k giebt es keine Relationen zwischen den $c_{\lambda\mu\nu}$, und jede symmetrische ganze Function lässt sich in diesem Falle daher nur auf Eine Art durch die elementaren symmetrischen Functionen darstellen. Unsere früheren Formeln, z. B. (14), zeigen somit, dass diese Darstellung nicht nothwendig eine ganzzahlige wird. Bisher wäre die Möglichkeit noch denkbar gewesen, dass mit Hülfe bestehender Relationen auch ganzzahlige Ausdrücke zu erreichen gewesen wären.

§ 386. Genau in derselben Art wie in § 123 ff. Bd. I partielle Differentialgleichungen für die symmetrischen Functionen einer Grössenreihe aufgestellt worden sind, so kann dies hier bei denen von mehreren, z. B. drei Grössenreihen geschehen. Wir wollen wenigstens den einfachsten Fall hier besprechen. Statt $x_\alpha, y_\alpha, z_\alpha$ setzen wir $x_\alpha + t$, $y_\alpha + t$, $z_\alpha + t$ bei $\alpha = 1, 2, \cdots k$ ein. Dadurch gehen, wie man leicht erkennt,

$c_{\alpha\beta\gamma}$ in $c_{\alpha\beta\gamma} + (k+1-\alpha-\beta-\gamma)[c_{\alpha-1,\beta,\gamma} + c_{\alpha,\beta-1,\gamma} + c_{\alpha,\beta,\gamma-1}]\cdot t + \cdots,$

$s_{\alpha\beta\gamma}$ in $s_{\alpha\beta\gamma} + [\alpha s_{\alpha-1,\beta,\gamma} + \beta s_{\alpha,\beta-1,\gamma} + \gamma s_{\alpha,\beta,\gamma-1}]\cdot t + \cdots,$

und, wenn R eine beliebige symmetrische Function der x, y, z bedeutet,

$$R \quad \text{in} \quad R + \sum_\alpha \left[\frac{\partial R}{\partial x_\alpha} + \frac{\partial R}{\partial y_\alpha} + \frac{\partial R}{\partial z_\alpha}\right] t + \cdots$$

über. Hierbei haben wir nur die Glieder ohne t und die mit t^1 hingeschrieben. Denkt man sich nun R gleichzeitig durch die x, y, z, ferner durch die $c_{\alpha\beta\gamma}$ und endlich durch die $s_{\alpha\beta\gamma}$ ausgedrückt und entwickelt dann nach der Substitution nach Potenzen von t, dann folgt in allen drei Ausdrücken die Gleichheit der entsprechenden Coefficienten der Potenzen von t, und so hat man für t^1 die Gleichungen

$$\begin{aligned}
&\sum_\alpha \left(\frac{\partial R}{\partial x_\alpha} + \frac{\partial R}{\partial y_\alpha} + \frac{\partial R}{\partial z_\alpha}\right) \\
&= \sum_{\alpha,\beta,\gamma} (k+1-\alpha-\beta-\gamma)\frac{\partial R}{\partial c_{\alpha\beta\gamma}}\cdot[c_{\alpha-1,\beta,\gamma} + c_{\alpha,\beta-1,\gamma} + c_{\alpha,\beta,\gamma-1}] \\
&= \sum_{\alpha,\beta,\gamma} \frac{\partial R}{\partial s_{\alpha\beta\gamma}}[\alpha s_{\alpha-1,\beta,\gamma} + \beta s_{\alpha,\beta-1,\gamma} + \gamma s_{\alpha,\beta,\gamma-1}].
\end{aligned}$$

Hierzu ist zu bemerken, dass $c_{000} = 1$, $s_{000} = k$, und dass Grössen c oder s mit negativen Indices gleich Null zu setzen sind. Prüft man diese Formel z. B. an

$$\sum x_1 y_2 z_3 = c_{111} = s_{100}s_{010}s_{001} - s_{100}s_{011} - s_{010}s_{101} - s_{001}s_{110} + 2s_{111},$$

so folgt

$$(k-2)[Sx_1y_2 + Sy_1z_2 + Sz_1x_2] = (k-2)[c_{011} + c_{101} + c_{110}]$$
$$= k(s_{010}s_{001} - s_{011}) + \cdots - s_{001}(s_{010} + s_{100}) - \cdots + 2(s_{011} + s_{101} + s_{110})$$
$$= (k-2)(s_{100}s_{010} + s_{010}s_{001} + s_{100}s_{001} - s_{110} - s_{101} - s_{011}),$$

was mit unseren früheren Resultaten übereinstimmt.

Siebenunddreissigste Vorlesung.

Resultante und Eliminante. Poisson'sche Methode.

§ 387. Wir wollen zunächst die Resultate der dreiunddreissigsten Vorlesung in etwas geänderter Bezeichnung derart reproduciren, dass wir statt zweier Gleichungen mit zwei Unbekannten m Gleichungen mit m Unbekannten betrachten. Für $m = 2$ kommen wir dann auf die bereits bewiesenen Sätze.

Es seien m allgemeine Gleichungen mit unbestimmten Coefficienten

$$(1) \qquad f_\alpha(z_1, z_2, \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

der m Unbekannten $z_1, z_2, \cdots z_m$ gegeben. Die Dimension von f_α sei gleich n_α. Das Product sämmtlicher Dimensionen setzen wir

$$(2) \qquad n_1 n_2 \cdots n_m = k.$$

Die Coefficienten von f_α mögen mit $a'_\alpha, a''_\alpha, \cdots$ und generell mit a_α bezeichnet werden. Jedem der a_α legen wir ein solches Gewicht bei, dass, wenn $z_1, z_2, \cdots z_m$ die Gewichte 1 bekommen, f_α isobarisch vom Gewichte n_α wird.

Das Gleichungssystem (1) besitzt k Wurzeln

$$(1^a) \quad (z_{11}, z_{21}, \cdots z_{m1}), \quad (z_{12}, z_{22}, \cdots z_{m2}), \cdots (z_{1k}, z_{2k}, \cdots z_{mk}).$$

Alle diese kann man durch die Lösung einer einzigen Gleichung erlangen, indem man die Liouville'sche Methode anwendet. Setzt man nämlich die Substitution an:

$$x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_m z_m,$$

wobei die $\varkappa$ unbestimmte gewichtlose Parameter bedeuten, und bezeichnet

(3) $\quad x_\lambda = \varkappa_1 z_{1\lambda} + \varkappa_2 z_{2\lambda} + \cdots + \varkappa_m z_{m\lambda}, \qquad (\lambda = 1, 2, \cdots k),$

dann besteht für x eine Gleichung k^{ten} Grades

(4) $\quad \varrho_0 x^k - \varrho_1(\varkappa_1, \cdots) x^{k-1} + \varrho_2(\varkappa_1, \cdots) x^{k-2} - \cdots \pm \varrho_k(\varkappa_1, \cdots) = 0$

mit den Wurzeln (3). Hierin sind die Coefficienten $\varrho_0, \varrho_1, \cdots \varrho_k$ ganze Functionen sämmtlicher Reihen $a_1, a_2, \cdots a_m$, und zwar sind sie homogen in den a_α vom Grade $k : n_\alpha$; es ist ferner ϱ_0 von den Parametern $\varkappa_1, \varkappa_2, \cdots$ frei, während ϱ_μ eine homogene ganze Function μ^{ten} Grades der $\varkappa$ ist. Das Polynom in (4) ist isobarisch vom Gewichte k und also ϱ_0 isobarisch vom Gewichte 0, und ϱ_μ vom Gewichte μ.

Für allgemeine Functionen (1) ist ϱ_0 irreductibel (vgl. § 153, Bd. I). ϱ_0 ist die Resultante der m Gleichungen

(5) $\quad \varphi_\alpha\left(1, \frac{z_2}{z_1}, \frac{z_3}{z_1}, \cdots \frac{z_m}{z_1}\right) = 0 \qquad (\alpha = 1, 2, \cdots m),$

wenn φ_α den Complex der Glieder n_α^{ter}, d. h. höchster Dimension in f_α bedeutet. Diese Resultante wollen wir auch als **die Resultante der m homogenen Gleichungen**

(5ᵃ) $\quad \varphi_\alpha(z_1, z_2, \cdots z_m) = 0$

bezeichnen. Ihr Verschwinden ist charakteristisch dafür, dass das System (5ᵃ) Wurzeln hat, deren Coordinaten nicht sämmtlich verschwinden.

Aus (4) ergeben sich die elementaren symmetrischen Functionen der Wurzeln $(z_{11}, z_{21}, \cdots z_{m1}), \cdots$ als gebrochene Functionen der a in der Gestalt

$$c_{100\cdots} = \frac{\varrho_1'}{\varrho_0}, \quad c_{010\cdots} = \frac{\varrho_1''}{\varrho_0}, \quad \cdots \quad c_{200\cdots} = \frac{\varrho_2'}{\varrho_0}, \quad \cdots,$$

wobei die $\varrho_1', \varrho_1'', \cdots \varrho_2', \cdots$ eine sofort erkennbare Bedeutung haben. Jede ganze symmetrische isobarische Function der $(z_{11}, z_{21}, \cdots z_{m1}), \cdots$ kann als gebrochene isobarische Function gleichen Gewichtes in den a dargestellt werden, entweder durch Vermittelung der $c_{\alpha\beta\gamma\cdots}$ oder direct mit Hülfe unbestimmter Coefficienten. Denken wir uns, die Darstellung sei mit Hülfe der c geschehen, und es kämen in einem Gliede μ Factoren c vor; dann wäre der Nenner ϱ_0^μ. Diese μ Factoren liefern bei der Darstellung der Function durch die a mindestens μ Factoren in diesen Coefficienten, und zwar tritt dieser Minimalfall nur ein, wenn alle c von der Form $c_{100\cdots}, c_{010\cdots}, c_{001\cdots}$ sind. Hat umgekehrt die Darstellung einer ganzen symmetrischen Function der Wurzeln durch die a nicht mehr als ν Factoren a in jedem Gliede, dann ist der Nenner höchstens ϱ_0^ν. Dieser hat, wie ϱ_0 selbst, das Gewicht 0; folglich ist der Zähler von demselben Gewichte, wie die dargestellte Function.

§ 388. Für $m = 2$ sind diese Sätze bewiesen. Wir nehmen an, sie gelten für ein beliebiges m und wollen sie für $(m + 1)$ nachweisen. Dadurch ist dann ihre allgemeine Gültigkeit dargethan.

Zu diesem Zwecke nehmen wir noch eine neue Gleichung $g(z_1, z_2, \cdots z_m) = 0$ mit den Coefficienten b an. Die Dimension von g sei q, und den b mögen solche Gewichte beigelegt werden, dass jedes einzelne Glied von g das Gewicht q besitzt. Nun bilden wir das Product

$$(6) \qquad \prod g(z_{1\lambda}, z_{2\lambda}, \cdots z_{m\lambda}) \qquad (\lambda = 1, 2, \cdots k),$$

erstreckt über alle Wurzeln (2) von (1). Dieses Product nennen wir, ähnlich wie früher bei zwei Gleichungen mit einer Unbekannten, aber versehen mit einem Factor, der sogleich angegeben werden soll, die Resultante der Gleichungen $f_\alpha = 0$, $g = 0$, und wir bezeichnen es mit R. Das Verschwinden von (6) ist charakteristisch dafür, dass (1) und $g = 0$ gemeinsame Wurzeln besitzen. Die Bildung von (6) zeigt, dass das Product in den Coefficienten b homogen vom Grade k ist. Es ist ferner in den b, $z_{1\lambda}$, $z_{2\lambda}$, $\cdots z_{m\lambda}$ $(\lambda = 1, 2, \cdots k)$ isobarisch vom Gewichte kq, da jeder Factor isobarisch vom Gewichte q ist. Es ist endlich in den Wurzeln (2) symmetrisch. Wir drücken sämmtliche auftretenden symmetrischen Functionen durch die a als gebrochene Functionen aus; dabei kann nur eine Potenz von ϱ_0 in den Nenner treten; die höchste vorkommende Potenz sei ϱ_0^μ. Da bei allgemeinen Functionen ϱ_0 nicht verschwindet (vgl. (5) und (5ᵃ) wegen der Bedeutung von ϱ_0), so nehmen wir ϱ_0^μ als den eben erwähnten Factor und setzen

$$(7) \qquad R = R(f_1, \cdots f_m;\, g) = \varrho_0^\mu \prod g(z_{1\lambda}, z_{2\lambda}, \cdots z_{m\lambda}),$$

wobei die $f_1, \cdots f_m;\, g$ nach Art der Argumente hinter R gesetzt werden sollen, um complicirte Schreibweise zu vermeiden. Die Function g hat dabei eine Ausnahmestellung erhalten, da ja in der That aus der Definition die Vertauschbarkeit mit den f_λ noch nicht hervorgeht, während die f beliebig unter einander versetzt werden dürfen. (7) ist jetzt ganz in den a; das Gewicht hat sich, da ϱ_0 vom Gewichte 0 ist, durch die Multiplication mit ϱ_0^μ nicht geändert, und beträgt also auf die a, b statt auf die b; $z_1, z_2, \cdots z_m$ bezogen auch kq.

§ 389. Ersetzen wir eins der f, z. B. f_1, durch das Product $f_1' \cdot f_1''$ zweier allgemeiner Functionen, so gilt die Formel

$$(8) \qquad R(f_1' \cdot f_1'', f_2, \cdots, f_m;\, g) = R(f_1', \cdots f_m;\, g)\, R(f_1'', \cdots f_m;\, g).$$

Die Wurzeln des umgestalteten Systems (1) theilen sich nämlich in

zwei Sorten, in diejenigen $\zeta_{1\lambda}, \zeta_{2\lambda}, \cdots \zeta_{m\lambda}$, welche $f_1' = 0$, $f_2 = 0, \cdots$ $f_m = 0$ befriedigen, und in diejenigen $\xi_{1\lambda}, \xi_{2\lambda}, \cdots \xi_{m\lambda}$, welche $f_1'' = 0$, $f_2 = 0, \cdots f_m = 0$ befriedigen. Demnach ist

$$\prod g(z_{1\lambda}, z_{2\lambda}, \cdots z_{m\lambda}) = \prod g(\zeta_{1\lambda}, \zeta_{2\lambda}, \cdots \zeta_{m\lambda}) \prod g(\xi_{1\lambda}, \xi_{2\lambda}, \cdots \xi_{m\lambda}).$$

Die Coefficienten von f_1' und von f_1'' seien generell durch a_1' bezw. a_1'' bezeichnet. Drückt man dann die beiden Producte auf der rechten Seite als gebrochene Functionen der $a_1', a_2, \cdots$ bezw. der $a_1'', a_2, \cdots$ aus, dann möge im ersten Producte etwa ein $\varrho_0'^{\varepsilon}$ und im zweiten etwa ein $\varrho_0''^{\eta}$ als Hauptnenner auftreten. Macht man links die gleiche Operation und ergiebt sich dabei ϱ_0^{μ}, so muss dies ein Theiler von $\varrho_0'^{\varepsilon}\varrho_0''^{\eta}$ sein, da ja links der Hauptnenner nicht weiter gehoben werden kann, während dies rechts denkbar wäre. Aber auch das geht nicht an; denn ϱ_0', ϱ_0'' als Resultanten von Gleichungen mit $(m-1)$ Unbekannten sind der Annahme nach irreductibel; ϱ_0' kann sich aber, da im zweiten Producte keine a' vorkommen, nicht gegen Factoren dieses zweiten Products heben lassen. Gleiches gilt für ϱ_0''. Demnach muss sogar der Hauptnenner rechts gleich dem auf der linken Seite sein, und multiplicirt man beide fort, so gelangt man zu (8). —

Ersetzen wir ferner g durch das Product $g' \cdot g''$ zweier allgemeiner Functionen, bei denen die Summe der Dimensionen gleich q ist, so gilt die Formel

$$(9)\qquad R(f_1, f_2, \cdots f_m; g' \cdot g'') = R(f_1, f_2, \cdots; g') \cdot R(f_1, f_2, \cdots; g'').$$

Zuerst ist nämlich identisch

$$\prod g'(z_1, z_2, \cdots z_m) \cdot g''(z_1, z_2, \cdots z_m) = \prod g'(z_1, z_2, \cdots z_m) \cdot \prod g''(z_1, z_2, \cdots z_m).$$

Jedes der Producte wird durch Multiplication mit einer Potenz von ϱ_0 zu einer ganzen Function der a gemacht. Ist rechts $\varrho_0^{\varkappa}$ der für das erste Product und ϱ_0^{λ} der für das zweite nötige, so kann sich offenbar auch links für $\varrho_0^{\varkappa+\lambda}$ nichts fortheben. Durch Multiplication mit $\varrho_0^{\varkappa+\lambda}$ folgt also (9).

§ 390. Mit Hülfe der Formeln (8) und (9) können wir die Irreductibilität von R bei allgemeinen Coefficienten a und b nachweisen.

Gesetzt, für ein System allgemeiner f_α der Dimensionen n_α gäbe es ein allgemeines g der Dimension q, für welches R sich in Factoren zerlegen liesse, dann können wir q so klein als möglich gewählt denken, d. h. so, dass bei Festhaltung der f_α kein allgemeines g von niederer als der q^{ten} Dimension noch ein reductibles R besitzt. Es sei

$$(10)\qquad R = R_1 \cdot R_2,$$

wobei R_1 und R_2 ganze Functionen der a und der b bedeuten. Statt

der allgemeinen Function g setzen wir nun das Product zweier allgemeinen Functionen $g' \cdot g''$ ein, deren Dimensionszahlen die Summe q haben, und deren Coefficienten mit b' bezw. b'' bezeichnet werden. Dann werden die b in g durch bilineare Formen

$$(11) \qquad b = b'_\alpha \cdot b''_\beta + b'_{\alpha-1} \cdot b''_{\beta+1} + \cdots + b'_{\alpha+1} \cdot b''_{\beta-1} + \cdots$$

ersetzt werden. Trägt man alles dies in (9) ein, so entsteht

$$(10^a) \qquad R = R_1 \cdot R_2 = R(f_1, \cdots f_m; g') \cdot R(f_1, \cdots f_m; g'').$$

Der Annahme nach sind die beiden Factoren rechts irreductibel, da ihre Dimensionen kleiner als q sind. Es müssen also auch die beiden Factoren R_1 und R_2 irreductibel sein, und weiter etwa

$$R(f_1, \cdots f_m; g') = R_1, \qquad R(f_1, \cdots f_m; g'') = R_2.$$

Nun war in (10) R_1 wie R_2 Function der Coefficienten b; in (10^a) ist dafür eine Function der Grössen (11) eingetreten, so dass also in R_1 wie in R_2 die Grössen b'_α, b''_α vorkommen; links dagegen treten in den beiden letzten Gleichungen nur entweder die b' oder die b'' auf. Das ist ein Widerspruch, der nur dadurch gehoben werden kann, dass q nicht mehr in niedere Summanden zerlegt werden kann, d. h. dass $q = 1$ ist.

Genau entsprechend folgt unter Verwendung von (8), wenn wir jetzt die Dimensionen $n_2, n_3, \cdots n_m, q = 1$ festhalten und n_1 unter Wahrung der Zerlegungsmöglichkeit so klein als es angeht wählen, dass der Minimalwerth von n_1 gleich 1 wird. Das Gleiche gilt für alle n, und wenn also überhaupt die Function R für irgend ein System allgemeiner Functionen der Dimensionen $n_1, n_2, \cdots n_m, q$ zerlegbar ist, dann gilt dasselbe auch für die Resultante eines Systems allgemeiner linearer Functionen.

Berechnet man nun aus den ersten m linearen Gleichungen die m Unbekannten $z_1, \cdots z_m$ und setzt die erhaltenen Werthe in die $(m+1)^{\text{te}}$ Gleichung $g = 0$ ein, so erhält man die allgemeine Determinante von $(m+1)$ Reihen von Coefficienten. Diese ist aber irreductibel, wie sich durch Induction leicht ergiebt. Für zwei Elementenreihen ist es klar. Hat man es für ν Elementenreihen bewiesen, so ergiebt es sich auf nachstehende Art für $(\nu + 1)$ Reihen. Wir entwickeln die Determinante nach den Elementen einer Spalte. Da die Elemente derselben von einander unabhängig sind, so kann eine Zerfällung der Determinante nur dadurch eintreten, dass alle zu den Spaltenelementen gehörigen Adjuncten einen gemeinsamen Theiler besitzen. Der Voraussetzung nach sind sie irreductibel; sie müssten also übereinstimmen. Das ist unmöglich, weil je zwei immer eine besondere Elementenzeile haben.

Somit folgt schliesslich: Die durch (7) definirte Function R ist bei unbestimmten Coefficienten der Functionen f und g irreductibel.

Der hier eingehaltene Gedankengang ist etwas bequemer als der in § 153 Bd. I bei $m = 1$ benutzte.

§ 391. In der Definitionsgleichung (7) ist der Function g eine Ausnahmestellung den Functionen f_α gegenüber gewahrt. In der That ist es nicht ohne Weiteres klar, dass man ein f_α mit g vertauschen kann. Bei einer Variablen folgte das sehr leicht auf Grund der dort möglichen Factorenzerlegung.

Wir wollen nun mit Hülfe des Irreductibilitätssatzes die Gleichberechtigung auch hier beweisen. Das Verschwinden von (7) giebt die charakteristische Bedingung dafür, dass die $(m+1)$ Gleichungen $f_\alpha = 0$, $g = 0$ mindestens eine gemeinsame Wurzel besitzen. Vertauscht man ein f mit g, so entsteht eine Resultante R' von gleicher Eigenschaft. Verschwindet sonach die eine für irgend ein Werthsystem der Coefficienten, so verschwindet die andere für dasselbe. Nach § 346, (IX) stimmen also R und R' in ihren irreductiblen Theilern überein, und nach den Ergebnissen des vorigen Paragraphen sind sie demnach bis auf einen Zahlenfactor identisch.

Aus der Bedeutung von R folgt ferner, dass diese Function nicht identisch verschwindet, wenn die Coefficienten der Functionen allgemeine Grössen sind. Ja es reicht bereits aus, dass bei willkürlich gegebenen Coefficienten der f_α die Coefficienten von g unbestimmt bleiben, um das identische Verschwinden von R auszuschalten. Selbst wenn wir nur das absolute Glied in g variabel halten, genügt dies schon.

§ 392. Wir können jetzt die Bezeichnungen derart ändern, dass wir statt g schreiben f_{m+1}, den Grad q durch n_{m+1} ersetzen und die f nun gleichmässig in die Resultantenbezeichnung eingehen lassen. Dann ist bewiesen:

Die Function

$$(7^a) \quad R = R(f_1, f_2, \cdots f_{m+1}) = \varrho_0^\mu \prod_\alpha f_{m+1}(z_{1\alpha}, z_{2\alpha}, \cdots z_{m\alpha}) \qquad (\alpha = 1, 2, \cdots k)$$

ist die Resultante des Gleichungssystems

$$(12) \; f_1(z_1, z_2, \cdots z_m) = 0, \; f_2(z_1, z_2, \cdots z_m) = 0, \cdots f_{m+1}(z_1, z_2, \cdots z_m) = 0.$$

Die $z_{1\alpha}, z_{2\alpha}, \cdots z_{m\alpha}$ sind die Wurzeln des Gleichungssystems (1). Das Verschwinden von R ist charakteristisch für die Existenz einer gemeinsamen Wurzel von (12). R ist bei allgemeinen Functionen (12) irreductibel und nicht identisch Null; es ist homogen in den Coefficienten jeder Function aus (12)

von einem Homogeneïtätsgrade gleich dem Producte der Dimensionen aller übrigen m Gleichungen. Die f können beliebig angeordnet werden. R ist isobarisch vom Gewichte

$$l = n_1 n_2 \cdots n_{m+1},$$

welches also dem Producte sämmtlicher Dimensionen gleich ist. Die behauptete Gradzahl der Homogeneïtät hinsichtlich der Coefficienten der ersten Functionen folgt daraus, dass alle f_a gleichberechtigt sind.

Wir wollen nun auch noch den Exponenten μ bestimmen. Zu diesem Zwecke müssen wir etwas weiter ausholen.

Wir betrachten die symmetrische Function

$$(12)\quad S(z_{11}^{\alpha} z_{21}^{\beta} z_{31}^{\gamma} \cdots z_{12}^{a} z_{22}^{b} \cdots z_{13}^{\mathfrak{a}} \cdots) \qquad (\alpha + \beta + \cdots \geqq a + b + \cdots \geqq \mathfrak{a} + \cdots)$$

und stellen sie durch die Coefficienten von (4) dar

$$(12^a)\qquad = \frac{\Sigma\, d\, \varrho_0^h \varrho_1'^m \varrho_1''^n \cdots \varrho_2'^p \cdots}{\varrho_0^{\mu}},$$

wobei die ϱ_1', ϱ_1'', $\cdots$ ϱ_2', $\cdots$ die Coefficienten von x_1, x_2, $\cdots$ x_1^2, $\cdots$ in $\varrho_1, \varrho_2, \cdots$ sind, und ϱ_0^{μ} den Hauptnenner der Darstellung bedeutet. Statt z_{11}, z_{21}, $\cdots$ setzen wir $z_{11}t$, $z_{21}t$, $\cdots$, während die übrigen $z_{12}, z_{22}, \cdots$; $z_{13}, z_{23}, \cdots$ ungeändert bleiben. Dadurch erhält (4) eine Wurzel, die mit t zugleich ins Unendliche wächst. Berechnet man für (4) die elementaren symmetrischen Functionen der x_1, x_2, $\cdots$, so folgt

$$\frac{\varrho_1}{\varrho_0} = t\,[x_1 z_{11} + x_2 z_{21} + \cdots] + [x_1(z_{12} + z_{13} + \cdots) + \cdots],$$

$$\frac{\varrho_2}{\varrho_0} = t\,[x_1^2(z_{11}z_{12} + \cdots) + x_1 x_2 (z_{11} z_{22} + \cdots) + \cdots] + \cdots,$$

. . . .

d. h. alle diese Grössen werden linear in t. Für grosse t wird also (4) annähernd in

$$t^{-1} \cdot x^k - (x_1 z_{11} + x_2 z_{21} + \cdots) x^{k-1} + \cdots = 0$$

übergehen. Für unendlich grosse t wird die erste Darstellung der symmetrischen Function S als höchste Potenz von t liefern $t^{\alpha+\beta+\cdots}$; die zweite dagegen t^{μ}. Folglich ist $\mu = \alpha + \beta + \gamma + \cdots$, d. h. gleich der Maximalsumme der Exponenten, die zu gleichem oberen Index einer Wurzelcoordinatenreihe gehören.

Damit ist aber natürlich nicht gesagt, dass bei der gegebenen Darstellung (12^a) von (12) die Zahl der in einzelne Glieder eingehenden Factoren $\mu = \alpha + \beta + \cdots$ nicht übertreffen dürfe; denn dieser Werth von μ ist nur aus dem Hauptnenner hergeleitet, und dieser kann geringer sein als einzeln vorkommende Nenner.

Um diese letzte Bemerkung durch ein Beispiel zu erläutern, nehmen wir

$$z_{11}, z_{21}; \ z_{12}, z_{22}; \ z_{13}, z_{23} \quad \text{und} \quad S(z_{11}{}^2 z_{22} z_{23}).$$

Nach § 381, (14) ist die symmetrische Function S gleich

$$\frac{1}{3}\left\{c_{10}^2 c_{02} - c_{10} c_{01} c_{11} + c_{01}^2 c_{20} + 2 c_{10} c_{12} - \cdots\right\}$$

und es scheint hiernach, als ob bei den Substitutionen

$$c_{10} = \frac{\varrho_1'}{\varrho_0}, \quad c_{01} = \frac{\varrho_1''}{\varrho_0}, \quad c_{20} = \frac{\varrho_2'}{\varrho_0}, \quad c_{11} = \frac{\varrho_2''}{\varrho_0}, \quad c_{02} = \frac{\varrho_2'''}{\varrho_0}, \cdots$$

der Hauptnenner $\varrho_0{}^3$ auftreten müsste. Nach unserem Satze ist dies nicht der Fall; und in der That hebt sich aus dem Aggregate der ersten drei Klammerglieder ϱ_0 weg, und es bleibt nur $\varrho_0{}^2$ als Hauptnenner zurück, wie eine etwas umständliche Rechnung zeigt.

Den gewonnenen Satz, den Schläfli (Wiener Denkschr. 4 (1852) S. 7) aufstellt und auf andere Art beweist, können wir folgendermassen aussprechen: Wenn man

$$(12) \quad S(z_{11}^{\alpha} z_{21}^{\beta} z_{31}^{\gamma} \cdots z_{12}^{a} z_{22}^{b} \cdots z_{13}^{\mathfrak{a}} \cdots) \quad (\alpha + \beta + \cdots \geqq a + b + \cdots \geqq \mathfrak{a} + \cdots)$$

durch die ϱ ausdrückt, dann tritt als Hauptnenner auf $\varrho_0^{\alpha+\beta+\gamma+\cdots}$.

Vergleichen wir (12) mit der symmetrischen Function (7^a), in welcher jedes Glied höchstens zur Dimension n_{m+1} in den $z_{1\alpha}, z_{2\alpha}, \cdots$ aufsteigt, und in welcher diese Dimension auch wirklich von einigen Gliedern erreicht wird, dann folgt:

In (7^a) ist der Exponent $\mu = n_{m+1}$ zu setzen.

§ 393. Die Coefficientenreihen $a_1, a_2, \cdots a_{m+1}$ der Functionen $f_1, f_2, \cdots f_{m+1}$ waren bisher als unbestimmte Grössen angenommen, denen solche Gewichte beigelegt wurden, dass jeder Summand in f_α das Gewicht n_α hatte. In allen Functionen f ersetzen wir jetzt jeden Coefficienten a durch eine ganze Function einer neuen Variablen t mit allgemeinen unbestimmten Coefficienten a', derart, dass t bis zu einem Grade aufsteigt, welcher dem Gewichte des zu ersetzenden Coefficienten gleichkommt. Die Gewichte der a' werden wieder so bestimmt, dass auch die umgewandelte Function in Hinsicht auf die a', die $z_1, z_2, \cdots$ und auf t isobarisch wird und das Gewicht n_α besitzt. Die neuen Functionen bezeichnen wir mit

$$(13) \qquad f_\alpha(z_1, z_2, \cdots z_m, t) \qquad (\alpha = 1, 2, \cdots, m+1),$$

und wenn wir f_α nach den fallenden Dimensionen seiner Glieder in den z und t ordnen, dann sei

$$(14) \quad f_\alpha(z_1, z_2, \cdots z_m, t) = u_\alpha^{(n_\alpha)}(z_1, z_2, \cdots t) + u_\alpha^{(n_\alpha - 1)}(z_1, z_2, \cdots t) + \cdots,$$

so dass jeder in $u_\alpha^{(n_\alpha)}$ eingehende Coefficient a' das Gewicht 0, jeder in $u_\alpha^{(n_\alpha - 1)}$ eingehende das Gewicht 1 besitzt, u. s. w. Hierbei entsteht

$$(15) \qquad u_\alpha^{(n_\alpha)}\left(\frac{z_1}{t}, \frac{z_2}{t}, \cdots \frac{z_m}{t}, 1\right)$$

aus dem früheren $f_\alpha(z_1, z_2, \cdots z_m)$, wenn man die Variablen $z_1, z_2, \cdots$ durch $\frac{z_1}{t}, \frac{z_2}{t}, \cdots$ ersetzt und die Coefficienten a in die neuen a' überführt. (15) ist demnach auch eine allgemeine Function der Dimension n_α mit unbestimmten Coefficienten.

§ 394. Wir führen jetzt dieselben Umänderungen, welche von (1) auf (13) leiteten, auch in $R = R(f_1, \cdots f_{m+1})$ durch. Dabei entsteht eine ganze Function von t und den a', die wir mit $R(t)$ bezeichnen wollen. $R(t)$ möge die Eliminante der $(m+1)$ Gleichungen (13) heissen, genommen in Beziehung auf die Unbekannten z_1, $z_2, \cdots z_m$.

Jedes Glied in dem früheren R war ein Potenzproduct der Coefficienten a und hatte in ihnen das Gewicht $l = n_1 \cdot n_2 \cdots n_{m+1}$. Daraus folgt, dass in $R(t)$ jedes Glied von R eine Function von t mit Coefficienten a' hervorruft, welche bis zum Grade l aufsteigt. Es ist demgemäss t^l die höchste Potenz von t, die in $R(t)$ auftreten kann. Wir wollen den Complex dieser Glieder mit t^l berechnen. Wir kommen zu ihnen, wenn wir in jedem f_α jedes a_α (mit dem Gewichte μ) durch $a'_\alpha t^\mu$ ersetzen, wobei a'_α das Gewicht Null hat; denn dabei beschränken wir uns auf die höchsten Glieder. Dadurch bekommen wir aber offenbar nichts anderes statt f_α als dieselbe, durch Einführung des t in $z_1, z_2, \cdots z_m, t$ homogen gemachte Function mit den Coefficienten a'_α, also $u_\alpha^{(n_\alpha)}(z_1, z_2, \cdots t)$. Folglich bildet in $R(t)$ der Complex der Coefficienten von t^l die Resultante von

$$(16) \quad u_1^{(n_1)}\left(\frac{z_1}{t}, \cdots \frac{z_m}{t}, 1\right) = 0, \quad u_2^{(n_2)}\left(\frac{z_1}{t}, \cdots \frac{z_m}{t}, 1\right) = 0, \cdots.$$

Diese Resultante ist bei allgemeinen Coefficienten a' nicht identisch Null. Somit steigt $R(t)$ wirklich bis zum Grade l auf.

Die Resultante von (16) wollen wir auch als Resultante der homogenen Functionen

$$(17) \quad u_1^{(n_1)}(z_1, \cdots z_m, t) = 0, \quad u_2^{(n_2)}(z_1, \cdots z_m, t) = 0, \cdots$$

bezeichnen. Ihr Verschwinden giebt an, dass das System (17) ausser der banalen Lösung $z_1 = 0, \cdots z_m = 0, t = 0$ noch andere Lösungen besitzt. Wir schreiben diese Resultante auch

$$(18) \qquad R\left(u_1^{(n_1)}, u_2^{(n_2)}, \cdots u_{m+1}^{(n_{m+1})}\right).$$

Dann ist das leitende Glied von $R(t)$

$$R\left(u_1^{(n_1)},\ u_2^{(n_2)},\ \cdots\ u_{m+1}^{(n_{m+1})}\right)\cdot t^l.$$

Der Grad der Eliminante in t ist im Allgemeinen gleich dem Producte der Dimensionen der Gleichungen. Er wird nur dann geringer, wenn die Aggregate (17) der Glieder höchster Dimension gleich Null gesetzt ein Gleichungssystem ergeben, welches ausser $(0, 0, \cdots 0)$ noch andere Wurzeln besitzt. Zu jeder Wurzel t_λ von $R(t) = 0$ giebt es Werthe $z_{1\lambda}, z_{2\lambda}, \cdots z_{m\lambda}$, für welche alle $f_\alpha = 0$ befriedigt werden. Ein allgemeines System hat also mindestens l Wurzeln.

Bei der Bestimmung der zu einem t' gehörigen z' stösst man auf dieselben Schwierigkeiten, die schon bei zwei Gleichungen mit zwei Unbekannten auftraten. Auch hier lassen diese sich am einfachsten durch die Liouville'sche Substitution überwinden.

§ 395. Wir setzen, ähnlich wie früher,

$$x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_m z_m + \lambda t$$

und tragen in die Functionen f_α für t ein

$$t = \frac{x - \varkappa_1 z_1 - \varkappa_2 z_2 - \cdots - \varkappa_m z_m}{\lambda};$$

die Resultate multipliciren wir, um ganze Functionen zu gewinnen, mit passenden Potenzen von λ und schreiben sie dann

(19) $$g_\alpha(z_1, z_2, \cdots z_m, x) = 0 \qquad (\alpha = 1, 2, \cdots, m+1).$$

Die Dimensionen von f_α und g_α sind die gleichen.

Aus (19) eliminiren wir die z und bilden die Eliminante

(20) $$R(x) = R(g_1, g_2, \cdots g_{m+1}) = 0.$$

Nun sei x_1 eine Wurzel von $R(x) = 0$. Dann haben die

$$g_\alpha(z_1, z_2, \cdots z_m, x_1) = 0 \qquad (\alpha = 1, 2, \cdots m+1)$$

eine gemeinsame Wurzel $z_{11}, z_{21}, \cdots z_{m1}$, und also besitzen wegen der Herkunft der g auch die

(13) $$f_\alpha(z_1, z_2, \cdots z_m, t) = 0$$

eine gemeinsame Wurzel, nämlich

$$z_1 = z_{11},\quad z_2 = z_{21},\quad \cdots\quad z_m = z_{m1},\quad t = \frac{x_1 - \varkappa_1 z_{11} - \cdots - \varkappa_m z_{m1}}{\lambda}.$$

Da diese Werthe ihrer Bedeutung nach von den Parametern $\varkappa_1, \cdots \varkappa_m, \lambda$ unabhängig sind, so folgt wie in § 358, dass jede Wurzel von (20) die Form $x_1 = \varkappa_1 z_{11} + \varkappa_2 z_{21} + \cdots + \lambda t_1$ besitzt, wobei $z_{11}, z_{21}, \cdots t_1$ die Coordinaten einer Wurzel von (13) sind. Hat man sämmtliche Wurzeln $x_1, x_2, \cdots$ von (19), so geben diese nach dem

angegebenen Verfahren sämmtliche Wurzeln von (13). Es giebt also im allgemeinen Falle so viele Wurzeln, als das Product der Dimensionen der Gleichungen beträgt.

Die Gleichung (20) dient ferner dazu, die elementaren symmetrischen Functionen der $x_1, x_2, \cdots$, und daraus nach § 377 die symmetrischen Functionen der Wurzeln von (13) zu berechnen.

§ 396. Wir setzen die Eliminante (20) in die Form

$$(21)\quad R(x) = \varrho_0(\varkappa_1, \cdots \lambda) \cdot x^l - \varrho_1(\varkappa_1, \cdots \lambda) \cdot x^{l-1} + \varrho_2(\varkappa_1, \cdots \lambda) \cdot x^{l-2} - \cdots.$$

Die Wurzeln von (21) sind von der Form $\varkappa_1 z_{11} + \cdots + \varkappa_m z_{m1} + \lambda t_1$, wo $z_{11}, z_{21}, \cdots t_1$ endliche Grössen sind. Es kann also für kein endliches Werthesystem $\varkappa_1, \varkappa_2, \cdots \varkappa_m, \lambda$ ein x_α unendlich gross werden. Dies müsste aber geschehen, wenn irgend eine Wurzel $(\varkappa_1', \varkappa_2', \cdots \varkappa_m', \lambda')$ von $\varrho_0 = 0$ nicht zugleich Wurzel aller $\varrho_1 = 0$, $\varrho_2 = 0$, $\cdots$ wäre. Man kann also wie in § 360 schliessen, dass ϱ_0 von $\varkappa_1, \cdots \lambda$ unabhängig gemacht werden kann, und dann durch $\varkappa_1 = 0, \cdots \varkappa_m = 0$, $t = 1$, dass ϱ_0 den Werth (18) hat.

Da die Wurzeln von (21) die Form $\varkappa_1 z_{11} + \varkappa_2 z_{21} + \cdots + \varkappa_m z_{m1} + \lambda t_1$ haben, und da

$$\frac{\varrho_1(\varkappa_1, \cdots \lambda)}{\varrho_0(\varkappa_1, \cdots \lambda)} = S(\varkappa_1 z_{1\mu} + \varkappa_2 z_{2\mu} + \cdots + \lambda t_\mu),$$

. . . .

so folgt, dass ϱ_α eine homogene Function α^{ten} Grades in den $\varkappa_1, \cdots \varkappa_m, \lambda$ ist. Man sieht, dass alle bei $m = 1$ gemachten Schlüsse sich hier wiederholen. Die Sätze aus § 360 können direct übernommen werden. So können wir sagen: In (21) ist ϱ_α homogen in den Parametern vom Grade α. Verschwinden für besondere Werthe der Coefficienten a die Grössen $\varrho_0, \varrho_1, \cdots \varrho_{\mu-1}$ identisch, d. h. für alle Werthe der Parameter, dann ist jeder von den Parametern abhängige Factor von ϱ_μ in jedem folgenden $\varrho_{\mu+1}$, $\varrho_{\mu+2}, \cdots$ als Theiler enthalten, so dass in der Eliminantengleichung jeder solche Theiler fortgehoben werden kann. Das Gewicht von ϱ_α in den Coefficienten a beträgt α. Auch dies folgt sofort aus der Form und dem Gewichte der Wurzeln.

Mit diesen Sätzen ist Alles für $(m + 1)$ bewiesen, was zu Beginn der Vorlesung für m angenommen und früher für $m = 2$ als richtig erkannt worden ist. Das Hauptproblem der Elimination ist damit erledigt. Die dazu benutzte Methode stammt von Poisson, Mémoire sur l'élimination dans les équations algébriques; Journ. de l'École polytechnique; IV; cahier 11, p. 199, der sie selbst als eine Erweiterung der von G. Cramer für zwei Gleichungen mit zwei Unbekannten ge-

gebenen in der Einleitung seiner Abhandlung erklärt. Das Theorem über die Zahl der Wurzeln war früher von **Bézout** aufgestellt und führt seinen Namen. Wir kommen auf diese Untersuchungen noch zurück.

§ 397. Von einer Wurzel x_1 der Gleichung (20) können wir durch die Annahme $x_1 = 1$, $x_2 = 0$, $\cdots \lambda = 0$ zu z_{11}, durch $x_1 = 0$, $x_2 = 1$, $x_3 = 0$, $\cdots \lambda = 0$ zu z_{21}, u. s. w. gelangen. Der Uebergang kann auch auf folgende analytische Art geschehen. Wir bilden ein System von l Gleichungen, die in den $z_{11}, z_{12}, z_{13}, \cdots z_{1l}$ linear sind

$$\begin{aligned} z_{11} \quad &+ z_{12} \quad + \cdots = S_0, \\ z_{11}x_1 \; &+ z_{12}x_2 \; + \cdots = S_1, \\ z_{11}x_1^2 &+ z_{12}^2 x_2 + \cdots = S_2, \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

Die rechten Seiten sind als symmetrische Functionen der Wurzeln bekannt. Die Determinante der linken Seite ist von Null verschieden, da die $x_1, x_2, \cdots$ von einander verschieden sind. Das ist leicht einzusehen. Wäre nämlich im allgemeinen Falle bei unbestimmten Coefficienten stets Wurzelgleichheit vorhanden, dann müsste dies auch in jedem besonderen Falle eintreten, während doch z. B.

$$f_1 \equiv z_1^{n_1} - 1 = 0, \quad f_2 \equiv z_2^{n_2} - 1 = 0, \quad \cdots f_{m+1} \equiv t^{n_{m+1}} - 1 = 0$$

keine gleichen Wurzeln x liefern werden. Das System der linearen Gleichungen kann daher aufgelöst werden, und so entsteht

$$z_{1\lambda} = T(x_\lambda) \qquad (\lambda = 1, 2, 3, \cdots l).$$

Das Gleiche lässt sich auch in folgender Art bewerkstelligen*). Der Ausdruck

$$R(y) \sum_\lambda \frac{z_{1\lambda}}{y - x_\lambda} = H(y)$$

ist eine ganze Function von y, deren Coefficienten symmetrische Functionen und somit bekannt sind. Setzt man $y = x_\lambda$, so entsteht, weil links nur ein Glied zurückbleibt,

$$z_{1\lambda} = \frac{H(x_\lambda)}{R'(x_\lambda)}. \tag{22}$$

Auf dieselbe Art findet man die $z_{2\lambda}$. Man kann also den Uebergang von den x_λ zu den $z_{\alpha\lambda}$ auf rein analytischem Wege durchführen.

---

*) Diese einfache Methode stammt wohl von **Kronecker** (J. f. M. 91, p. 307).

Achtunddreissigste Vorlesung.

Unendlich grosse Wurzeln. Vielfache Wurzeln. Unendlich viele Wurzeln.

§ 398. Wenn ein allgemeines System von m Gleichungen mit m Unbekannten gegeben ist, so kann man den unbestimmten Coefficienten, wie wir gesehen haben, stets solche besonderen Werthe ertheilen, dass auch das neue besondere System $k = n_1 \cdot n_2 \cdots n_m$ Lösungen besitzt. Liegt nun ferner irgend ein System von m Gleichungen mit k_1 ($< k$) Lösungen vor, so kann der Uebergang von der ersten Eliminante zur zweiten nur dadurch geschehen, dass $\varrho_0, \varrho_1, \cdots \varrho_{k-k_1-1}$ gleich Null werden; es giebt dann also $(k - k_1)$ Wurzeln x, die ins Unendliche gewachsen sind, und also auch, falls die Gleichungen präparirt waren, ebensoviele Wurzeln $(z_1, z_2, \cdots z_m)$, deren Coordinaten sämmtlich ∞ geworden sind. In dem einfachsten Falle $k_1 = (k - 1)$ wird nur $\varrho_0 = 0$ oder

$$R\left(\frac{z_1}{z_m}, \frac{z_2}{z_m}, \cdots \frac{z_{m-1}}{z_m}, 1\right) = 0,$$

d. h. die homogenen Gleichungen, welche entstehen, wenn man in allen f_α die Glieder höchster, n_α^{ter} Dimension gleich Null setzt, haben eine gemeinsame Lösung. Die Verhältnisse sind hier also genau denen analog, welche wir bei zwei Gleichungen mit zwei Unbekannten besprochen haben. Schon Euler*) nimmt bei der Zählung der Wurzeln Rücksicht auf solche unendlichen Wurzeln.

Es ist vielleicht nicht unangebracht, folgende, freilich naheliegende Bemerkung zu machen. Es mögen $q_{\alpha,\beta}$ beliebige ganze Functionen der $z_1, \cdots z_m$ bedeuten; dann sind die beiden Systeme

$$(1) \qquad f_1 = 0, \quad f_2 = 0, \cdots f_m = 0$$

und

$$f_1 = 0, \quad f_2 + q_{2,1} f_1 = 0, \quad f_3 + q_{3,2} f_2 + q_{3,1} f_1 = 0, \cdots,$$
$$f_m + q_{m,m-1} f_{m-1} + \cdots + q_{m,2} f_2 + q_{m,1} f_1 = 0$$

insofern einander äquivalent, als jede endliche Lösung des einen der beiden Systeme auch das andere befriedigt, wie leicht zu sehen ist. Gleichwohl können die Gradzahlen der Gleichungen des zweiten Systems beliebig erhöht auftreten. Dies erklärt sich dadurch, dass das zweite System eine Reihe unendlich grosser Wurzeln hat, die dem ersten fehlen.

---

*) Mém. de l'Acad. de Berlin (1748), p. 234.

§ 399. Wir gehen jetzt zur Betrachtung **mehrfacher Wurzeln** über. Bei allgemeinen Gleichungen können solche nicht auftreten, denn das Gleiche müsste sonst auch in jedem besonderen Falle gewahrt bleiben, während sich ja leicht Beispiele aufstellen lassen, in denen keine mehrfachen Wurzeln vorhanden sind, vgl. S. 87.

Besitzt die Eliminante $R(x) = 0$ den Wert $x = x_1$ als α-fache Wurzel, dann wollen wir das zugehörige $(z_{11}, z_{21}, \cdots z_{m1})$ gleichfalls als α-fache Wurzel auffassen. Durch Berücksichtigung der unendlichen und der vielfachen Wurzeln erst wird der Bézout'sche Satz von der Anzahl der Wurzeln jedes Systems von Gleichungen richtig, falls nicht der später zu besprechende Fall unendlich vieler Wurzeln eintritt.

Wir wollen noch von einer anderen Seite her die mehrfachen Wurzeln zu behandeln suchen. Wir setzen, indem wir unter $\zeta_1, \cdots \zeta_m$ beliebige aber feste Werte verstehen,

$$(2)\qquad z_1 = \zeta_1 + \varrho u_1, \quad z_2 = \zeta_2 + \varrho u_2, \cdots z_m = \zeta_m + \varrho u_m; \\ (u_1^2 + u_2^2 + \cdots + u_m^2 = 1).$$

Dann gehört zu jedem Werthsysteme $u_1, u_2, \cdots u_m; \varrho$ ein einziges System $z_1, z_2, \cdots z_m$; umgekehrt gehören zu jedem Werthsystem $z_1, z_2, \cdots z_m$ die beiden Werthsysteme

$$\varrho = \pm\sqrt{(z_1 - \zeta_1)^2 + \cdots + (z_m - \zeta_m)^2}; \quad u_1 = \frac{z_1 - \zeta_1}{\varrho},\ u_2 = \frac{z_2 - \zeta_2}{\varrho}, \cdots$$

ausgenommen zu $z_1 = \zeta_1, z_2 = \zeta_2, \cdots z_m = \zeta_m$, welchem $\varrho = 0$; $(u_1, u_2, \cdots$ beliebig) entspricht. Trägt man (2) in (1) ein, so erhält man, wenn $(\zeta_1, \cdots \zeta_m)$ keine Wurzel von (1) bedeutet, ein Gleichungssystem von $(m + 1)$ Gleichungen mit $(m + 1)$ Unbekannten und nach dem eben Dargelegten mit doppelter Zahl der endlichen Wurzeln gegenüber (1). Beschränkt man aber die Systeme auf positive ϱ, so entspricht jeder Wurzel von (1) eine solche von (2) und umgekehrt.

Wir wollen jetzt $(\zeta_1, \zeta_2, \cdots \zeta_m)$ gleich einer Wurzel von (1) setzen. Dann ist

$$(3)\quad f_\alpha = \varrho\left[u_1\frac{\partial f_\alpha}{\partial \zeta_1} + \cdots + u_m\frac{\partial f_\alpha}{\partial \zeta_m}\right] + \varrho^2 \cdot G_\alpha = 0 \qquad (\alpha = 1, 2, \cdots m),$$

wenn unter $\frac{\partial f_\alpha}{\partial \zeta_\beta}$ das Resultat der Substitution von $(\zeta_1, \zeta_2, \cdots \zeta_m)$ in $\frac{\partial f_\alpha}{\partial z_\beta}$ verstanden wird, und G_α eine nach Potenzen von ϱ aufsteigende Function bedeutet. Unterdrücken wir in (3) den Factor ϱ, so müssen

$$(3^a)\quad \left[u_1\frac{\partial f_\alpha}{\partial \zeta_1} + \cdots + u_m\frac{\partial f_\alpha}{\partial \zeta_m}\right] + \varrho \cdot G_\alpha = 0 \qquad (\alpha = 1, 2, \cdots m)$$

von allen übrigen Wurzelsystemen u, ϱ, die aus den übrigen Wurzelsystemen $(z_{1\lambda}, z_{2\lambda}, \cdots z_{m\lambda})$ entspringen, befriedigt werden; und umgekehrt folgt aus jedem Wurzelsystem u, ϱ ein solches $(z_{1\lambda}, z_{2\lambda}, \cdots z_{m\lambda})$. Wir wollen unter Wahrung der Wurzel $(z_{11}, z_{21}, \cdots) = (\zeta_1, \zeta_2, \cdots)$ die Coefficienten von (1) so abändern, dass eine zweite Wurzel $(z_{12}, z_{22}, \cdots z_{m2})$ der ersten sich unendlich nähert. Dann wird das zugehörige ϱ gleich 0 werden; und sonach muss es Werthe u_λ geben, die das lineare System der m homogenen Gleichungen

$$u_1 \frac{\partial f_\alpha}{\partial \zeta_1} + u_2 \frac{\partial f_\alpha}{\partial \zeta_2} + \cdots + u_m \frac{\partial f_\alpha}{\partial \zeta_m} = 0 \qquad (\alpha = 1, 2, \cdots m)$$

befriedigen. Es wird demgemäss die Determinante

$$J = \left| \frac{\partial f_\lambda}{\partial \zeta_\mu} \right| \qquad (\lambda, \mu = 1, 2, \cdots m)$$

gleich Null sein. J ist die von Jacobi eingeführte Functionaldeterminante, auf deren Bedeutung für die Elimination wir später noch genauer eingehen werden. Ist umgekehrt $J = 0$, und bezeichnet $u_1', u_2', \cdots u_m'$ eine Lösung von (4), für welche $\sum u_\lambda'^2 = 1$ ist, dann folgt aus ihr und $\varrho = 0$ eine Lösung von (3ᵃ); d. h. (3) besitzt noch eine zweite Wurzel $\varrho = 0$. Daher ist $J = 0$ charakteristisch dafür, dass die Wurzel $(\zeta_1, \cdots \zeta_m)$ des Systems (1) mindestens von der Multiplicität 2 ist.

Die Behandlung vielfacher Wurzeln höherer Multiplicität nach derselben Methode ist schwierig, da zu einem $\varrho = 0$ verschiedene Systeme u gehören können, durch welche mehrere der in (3) rechts stehenden Anfangsglieder verschwinden.

§ 400. Ein anderer wichtiger Satz über mehrfache Wurzeln bedarf zu seiner Ableitung einiger Vorbereitungen.

Wir wollen annehmen, jedem Summanden einer Summe sei ein beliebiges Gewicht beigelegt worden. Unter dem unteren Grenzgewichte oder kürzer dem Grenzgewichte der Summe, (da wir mit anderen in der Folge nicht zu thun haben), wollen wir ein Gewicht verstehen, unter welches kein Gewicht eines der Summanden sinken kann, welches aber auch wirklich das niedrigste vorkommende Gewicht eines der vorhandenen Summanden ist. Der Einfachheit halber beschränken wir uns von vornherein auf nicht negative Gewichte und Grenzgewichte. Bezeichnen wir nun mit $g_1, g_2, \cdots g_n$ die Grenzgewichte einer Reihe $u_1, u_2, \cdots u_n$ von einander unabhängiger Grössen, wobei die u so angeordnet sind, dass $g_1 \leq g_2 \leq \cdots \leq g_n$

ist, dann hat $S(u_1)$ als Grenzgewicht offenbar g_1; ebenso $S(u_1 u_2)$ als Grenzgewicht $g_1 + g_2$, u. s. w. Daraus folgt, dass die Coefficienten von

$$u^n - a_1 u^{n-1} + a_2 u^{n-2} - \cdots = (u - u_1)(u - u_2) \cdots (u - u_n) = 0$$

der Reihe nach die Grenzgewichte $\gamma_0 = 0$, $\gamma_1 = g_1$, $\gamma_2 = g_1 + g_2, \cdots$ haben. Dieser Satz lässt sich auch umkehren. Hat a_1 das Grenzgewicht γ_1, so muss dieses, da $a_1 = S(u_1)$ ist, Grenzgewicht eines der u sein, und zwar das kleinste vorkommende. Da ferner $a_2 = S(u_1 u_2)$ ist, so wird das nächst grössere Grenzgewicht eines u gleich $(\gamma_2 - \gamma_1)$ sein, u. s. f. bis zu $\gamma_n - \gamma_{n-1}$. Wird somit eine symmetrische Function $S(u_1^{p_1} u_2^{p_2} \cdots u_n^{p_n})$ mit $p_1 \geqq p_2 \geqq \cdots p_n$ im Anschlusse an die letzte Gleichung gebildet, so ist deren Grenzgewicht, durch die Grenzgewichte der Coefficienten ausgedrückt,

$$p_1 g_1 + p_2 g_2 + \cdots + p_n g_n = p_1 \gamma_1 + p_2(\gamma_2 - \gamma_1) + \cdots + p_n(\gamma_n - \gamma_{n-1}).$$

§ 401. Von diesen allgemeinen Sätzen wollen wir wichtige Anwendungen machen. Es seien die beiden Gleichungen gegeben

$$(6)\quad f_1(z_1) = a_r z_1^r + a_{r-1} z_1^{r-1} + \cdots + a_\varrho z_1^\varrho + a_{\varrho-1} z_1^{\varrho-1} + \cdots + a_0 = 0,$$

$$(7)\quad f_2(z_1) = b_s z_1^s + b_{s-1} z_1^{s-1} + \cdots + b_\sigma z_1^\sigma + b_{\sigma-1} z_1^{\sigma-1} + \cdots + b_0 = 0.$$

Hier ertheilen wir den $a_r, a_{r-1}, \cdots a_\varrho$; $b_s, b_{s-1}, \cdots b_\sigma$ die Grenzgewichte Null, den folgenden $a_\varkappa$, $b_\varkappa$ die Grenzgewichte $\varrho - \varkappa$, $\sigma - \varkappa$, so dass insbesondere a_0 das Grenzgewicht ϱ, und b_0 das Grenzgewicht σ hat. Dann haben ϱ der Wurzeln $z_{11}, z_{12}, \cdots z_{1\varrho}$ von (6) das Grenzgewicht 1, und die übrigen $(r - \varrho)$ das Grenzgewicht 0, wie aus § 400 folgt. Es hat ferner die symmetrische Function

$$S(z_{11}^{p_1} z_{12}^{p_2} \cdots z_{1r}^{p_r}) \qquad (p_1 \geqq p_2 \geqq \cdots \geqq p_r)$$

das Grenzgewicht $p_{r-\varrho+1} + p_{r-\varrho+2} + \cdots + p_r$.

Wir bilden nun die Resultante von (6) und (7)

$$(8)\quad f_2(z_{11}) f_2(z_{12}) \cdots = \prod [b_s z_{1\lambda}^s + \cdots + b_\sigma z_{1\lambda}^\sigma + b_{\sigma-1} z_{1\lambda}^{\sigma-1} + \cdots + b_0]$$

und suchen für sie das Grenzgewicht zu bestimmen. Die einzelnen Summanden des ausgeführten Products haben die Form

$$(9)\qquad b_\alpha b_\beta b_\gamma \cdots S(z_{11}^\alpha z_{12}^\beta z_{13}^\gamma \cdots).$$

Die Summanden der einzelnen Factoren rechts in (8) zerlegen wir in zwei Theile; die ersten erstrecken sich vom Anfangsgliede bis $b_\sigma z_{1\lambda}^\sigma$, die zweiten vom folgenden Gliede bis zu Ende. Tritt in einen Summanden der Form (9) ein Glied der ersten Art ein (etwa $\alpha > \sigma$), so wird das Grenzgewicht sicher nicht vermehrt, wenn man dieses Glied durch das entsprechende $b_\sigma z_{11}^\sigma$ ersetzt; denn das alte wie das neue b haben das Grenzgewicht 0, und der Exponent von z_{11}, der möglicher-

weise beim Grenzgewichte mitbestimmend auftritt, vermindert sich. Kommt ferner ein Glied der zweiten Art in (9) vor (etwa $\beta < \sigma$), so wird das Grenzgewicht des Summanden sicher nicht vermehrt, wenn auch dieses Glied durch das entsprechende $b_\sigma z_{12}^\sigma$ ersetzt wird. Denn der Exponent von z_{12}, der möglicherweise mitbestimmend wirkt, wird nur um so viele Einheiten erhöht, als das Grenzgewicht des b, welches sicher Einfluss besitzt, sich vermindert. Daraus folgt, dass

$$(9^a) \qquad (b_\sigma)^r S(z_{11} z_{12} \cdots z_{1r})^\sigma$$

das niedrigste Grenzgewicht hat; d. h. ϱ^σ ist das Grenzgewicht der Resultante. Dieses Resultat hätte sich kürzer aus § 360 herleiten lassen; die weiteren nothwendigen Folgerungen wären aber auf dem dort eingeschlagenen Wege nicht zu erhalten gewesen.

Unsere allgemeinen Annahmen über die Grenzgewichte werden durch die folgenden Festsetzungen nicht gestört. Wir nehmen

$$a_\varkappa = a_{\varkappa 0} + a_{\varkappa 1} z_2 + \cdots + a_{\varkappa, r-\varkappa} z_2^{r-\varkappa}, \quad b_\varkappa = b_{\varkappa 0} + b_{\varkappa 1} z_2 + \cdots + b_{\varkappa, s-\varkappa} z_2^{s-\varkappa},$$

schreiben statt f_1 und f_2 jetzt

$$(10) \qquad \begin{aligned} f_1(z_1, z_2) &= \sum a_{\varkappa\lambda} z_1^\varkappa z_2^\lambda = 0 \qquad (\varkappa + \lambda = 0, 1, \cdots r), \\ f_2(z_1, z_2) &= \sum b_{\varkappa\lambda} z_1^\varkappa z_2^\lambda = 0 \qquad (\varkappa + \lambda = 0, 1, \cdots s), \end{aligned}$$

und geben den $a_{\varkappa\lambda}$ $(\varkappa + \lambda \geqq \varrho)$ und den $b_{\varkappa\lambda}$ $(\varkappa + \lambda \geqq \sigma)$ die Grenzgewichte 0, jedem $a_{\varkappa\lambda}$ $(\varkappa + \lambda < \varrho)$ das Grenzgewicht $(\varrho - \varkappa - \lambda)$, und jedem $b_{\varkappa\lambda}$ $(\varkappa + \lambda < \sigma)$ das Grenzgewicht $(\sigma - \varkappa - \lambda)$; z_2 soll das Gewicht 1 haben.

Dann besitzt die Eliminante $R(z)$, sowie ihr absolutes Glied in den Coefficienten und in z_2 das Grenzgewicht $\varrho\sigma$. Dasselbe bleibt gültig, wenn wir vermittels der Liouville'schen Substitution, unter u_1, u_2 Parameter verstehend, $x = u_1 z_1 + u_2 z_2$ in (10) einführen und die Eliminante $R(x)$ berechnen. Setzen wir sie gleich Null,

$$x^{rs} + A_1 x^{rs-1} + A_2 x^{rs-2} + \cdots + A_{\varrho\sigma} x^{\varrho\sigma} + \cdots + A_{rs} = 0,$$

so folgt, dass $\varrho\sigma$ der Wurzeln x das Grenzgewicht 1 und die anderen das Grenzgewicht 0 haben. Gehen wir zu den z zurück, so finden wir, dass beide Coordinaten für $\varrho\sigma$ der Wurzeln $(z_{11}, z_{21}), \cdots$ das Grenzgewicht 1 haben, und dass bei den anderen die Grenzgewichte 0 auftreten. Folglich hat

$$(11) \qquad S(z_{11}^{p_1} z_{21}^{q_1} z_{12}^{p_2} z_{22}^{q_2} \cdots) \qquad (p_1 + q_1 \geqq p_2 + q_2 \geqq \cdots)$$

das Grenzgewicht

$$(11^a) \quad (p_{rs-\varrho\sigma+1} + q_{rs-\varrho\sigma+1}) + (p_{rs-\varrho\sigma+2} + q_{rs-\varrho\sigma+2}) + \cdots + (p_{rs} + q_{rs}).$$

Wir wollen hier gleich bemerken, dass wir für den Fall zweier Variablen das zu beweisende Theorem hierdurch schon als richtig erkannt haben, nämlich: Ertheilt man in (10) den Coefficienten solche Grenzgewichte, dass bei den Gewichten 1 für z_1 und z_2 das Grenzgewicht von f_1 gleich ϱ und das von f_2 gleich σ wird, dann haben die Coordinaten von $\varrho\sigma$ der Wurzeln des Systems $f_1 = 0$, $f_2 = 0$ die Grenzgewichte 1.

§ 402. Wir nehmen jetzt noch eine dritte Gleichung zu (10) hinzu:

$$(12) \qquad f_3(z_1, z_2) = \sum c_{\varkappa\lambda} z_1^\varkappa z_2^\lambda \qquad (\varkappa + \lambda = 0, 1, \cdots t)$$

und geben den $c_{\varkappa\lambda}$ $(\varkappa + \lambda \geqq \tau)$ die Grenzgewichte 0, den $c_{\varkappa\lambda}$ $(\varkappa + \lambda < \tau)$ die Grenzgewichte $(\tau - \varkappa - \lambda)$. Dann bilden wir wieder die Resultante

$$(13) \qquad f_3(z_{11}, z_{21}) f_3(z_{12}, z_{22}) \cdots f_3(z_{1,rs}, z_{2,rs}),$$

wobei die $(z_{1\lambda}, z_{2\lambda})$ die Wurzeln von (10) sind. Wir verfahren, um das Grenzgewicht von (13) zu berechnen, genau wie im vorigen Paragraphen, indem wir die Glieder von (12) in zwei Theile theilen, deren erster alle die enthält, bei denen $\varkappa + \lambda \geqq \tau$ ist. Tritt in einem Summanden des entwickelten Ausdrucks (13)

$$c_{\alpha\beta} c_{\gamma\delta} \cdots S(z_{11}^\alpha z_{21}^\beta z_{12}^\gamma z_{22}^\delta \cdots)$$

ein Summand des ersten Theiles auf, so kann man ihn ohne Erhöhung des Grenzgewichtes durch einen solchen ersetzen, bei dem $\varkappa + \lambda = \tau$ ist. Das Gleiche tritt im zweiten Falle auf, aus denselben Gründen wie oben, und so folgt, dass

$$c_{\varkappa\lambda}^{rs} (z_{11} z_{12} \cdots z_{1,rs})^\varkappa (z_{21} z_{22} \cdots z_{2,rs})^\lambda \qquad (\varkappa + \lambda = \tau)$$

das Grenzgewicht liefert. Nach (11^a) ist dies $\varrho\sigma(\varkappa + \lambda) = \varrho\sigma\tau$.

Unsere allgemeinen Annahmen über die Grenzgewichte werden durch die folgenden Festsetzungen nicht gestört. Wir nehmen

$$\begin{aligned} a_{\varkappa\lambda} &= a_{\varkappa\lambda 0} + a_{\varkappa\lambda 1} z_3 + \cdots + a_{\varkappa,\lambda,r-\varkappa-\lambda} z_3^{r-\varkappa-\lambda}, \\ b_{\varkappa\lambda} &= b_{\varkappa\lambda 0} + b_{\varkappa\lambda 1} z_3 + \cdots + b_{\varkappa,\lambda,s-\varkappa-\lambda} z_3^{s-\varkappa-\lambda}, \\ c_{\varkappa\lambda} &= c_{\varkappa\lambda 0} + c_{\varkappa\lambda 1} z_3 + \cdots + c_{\varkappa,\lambda,t-\varkappa-\lambda} z_3^{t-\varkappa-\lambda}, \end{aligned}$$

schreiben statt f_1, f_2, f_3 jetzt

$$(14) \qquad \begin{aligned} f_1(z_1, z_2, z_3) &= \sum a_{\varkappa\lambda\mu} z_1^\varkappa z_2^\lambda z_3^\mu = 0 \qquad (\varkappa + \lambda + \mu = 0, 1, \cdots r), \\ f_2(z_1, z_2, z_3) &= \sum b_{\varkappa\lambda\mu} z_1^\varkappa z_2^\lambda z_3^\mu = 0 \qquad (\varkappa + \lambda + \mu = 0, 1, \cdots s), \\ f_3(z_1, z_2, z_3) &= \sum c_{\varkappa\lambda\mu} z_1^\varkappa z_2^\lambda z_3^\mu = 0 \qquad (\varkappa + \lambda + \mu = 0, 1, \cdots t), \end{aligned}$$

und geben den $a_{\varkappa\lambda\mu}$ das Grenzgewicht $\varrho - (\varkappa + \lambda + \mu)$, falls diese Differenz positiv ist, sonst das Grenzgewicht 0; ähnlich verfahren wir

mit den $b_{\varkappa\lambda\mu}$, $c_{\varkappa\lambda\mu}$ und den $\sigma - (\varkappa + \lambda + \mu)$, $\tau - (\varkappa + \lambda + \mu)$; z_3 soll das Grenzgewicht 1 haben. Dann hat nach dem obigen Resultate die Eliminante $R(z_3)$ das Grenzgewicht $\varrho\sigma\tau$. Dasselbe bleibt bestehen, wenn wir vermittels der Liouville'schen Substitution $x = u_1 z_1 + u_2 z_2 + u_3 z_3$ einführen, für $R(x)$ und auch für ihr absolutes Glied. Daraus folgt dann, dass $\varrho\sigma\tau$ der Wurzeln von (14) in allen ihren Coordinaten z_1', z_2', z_3' die Grenzgewichte 1 besitzen. Folglich gelten, entsprechend modificirt, die obigen Sätze über symmetrische Functionen u. s. w.

In gleicher Weise können wir zu mehr Variablen aufsteigen. Unsere Methode zeigt uns also die Gültigkeit des allgemeinen Satzes: Geben wir den Coefficienten von

$$f_\lambda(z_1, z_2, \cdots z_m) = 0 \qquad (\lambda = 1, 2, \cdots m) \tag{15}$$

solche Grenzgewichte, dass jedes f_λ das Grenzgewicht ϱ_λ erhält, falls man allen z das Gewicht 1 beilegt, dann haben $\varrho_1 \cdot \varrho_2 \cdots \varrho_m$ der Wurzeln von (15) in allen ihren m Coordinaten das Grenzgewicht 1.

§ 403. Von diesem allgemeinen Satze machen wir eine Anwendung, indem wir alle diejenigen Coefficienten in jedem f_λ gleich Null setzen, deren zugehörige Potenzproducte geringere Dimension haben als ϱ_λ beträgt. Diese Coefficienten werden also bei der Berechnung der Gewichte ausgeschaltet. Die übrigen Coefficienten setzen wir constant. Tragen wir

$$x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_m z_m \tag{16}$$

ein, und berechnen die Eliminante $R(x)$, so ist deren Grenzgewicht auch $\varrho_1 \varrho_2 \cdots \varrho_m$; da aber alle vorkommenden Coefficienten ganze Functionen unserer Constanten sind, so ist dies nur möglich, wenn Glieder x^λ, bei denen $\lambda < \varrho_1 \varrho_2 \cdots \varrho_m$ ist, überhaupt nicht vorkommen. Das zeigt: Ist $(0, 0, \cdots 0)$ eine ϱ_λ-fache Wurzel von $f_\lambda = 0$ $(\lambda = 1, 2, \cdots m)$, dann ist $(0, 0, \cdots 0)$ eine $(\varrho_1 \varrho_2 \cdots \varrho_m)$-fache Wurzel des Systems (15).

Durch diesen Satz haben wir nur eine untere Grenze für die Multiplicität angegeben. Es lassen sich aber sofort Fälle construiren, für welche diese Grenze nicht überschritten wird; z. B. für

$$f_\lambda = z_\lambda^{n_\lambda} + c_1^{(\lambda)} z_\lambda^{n_\lambda - 1} + c_2^{(\lambda)} z_\lambda^{n_\lambda - 2} + \cdots + c_{n_\lambda - \varrho_\lambda}^{(\lambda)} z_\lambda^{\varrho_\lambda} \qquad (\lambda = 1, 2, \cdots m),$$

sobald die c Constanten sind, deren letzte von Null verschieden sein muss. Daraus schliessen wir: Das obige Theorem giebt die wahre Multiplicität im allgemeinen Falle.

Was von dem Specialpunkte $(0, 0, \cdots 0)$ bewiesen wurde, gilt, wie man durch Coordinatenverschiebung erkennt, für jeden beliebigen

Punkt $(q_1, q_2, \cdots q_m)$, so dass wir sagen können: Ist $(q_1, q_2, \cdots q_m)$ eine ϱ_λ-fache Wurzel der Gleichung $f_\lambda = 0$ $(\lambda = 1, 2, \cdots m)$, dann ist $(q_1, q_2, \cdots q_m)$ im allgemeinen Falle genau eine $(\varrho_1 \varrho_2 \cdots \varrho_m)$-fache Wurzel des Systems (15).

§ 404. Endlich wollen wir den Fall besprechen, dass unser System

$$(1)\quad f_1(z_1, z_2, \cdots z_m) = 0\,,\ f_2(z_1, z_2, \cdots z_m) = 0\,, \cdots f_m(z_1, z_2, \cdots z_m) = 0$$

unendlich viele Wurzeln $(z_1, z_2, \cdots z_m)$ zulässt. Die einzelnen Functionen von (1) mögen durch vorläufige Transformation bereits präparirt sein (§ 340, § 353, § 355), so dass etwaige Zufälligkeiten, die durch specielle Formen der f hervorgerufen werden, ausgeschlossen sind. Wir führen etwa an Stelle von z_m mittels der Liouville'schen Substitution die Grösse

$$(16)\qquad x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_m z_m$$

ein und bilden die Eliminante $R(x)$. Charakteristisch für das Vorhandensein unendlich vieler Wurzeln ist es, dass $R(x)$ identisch verschwindet; d. h. alle in R auftretenden Coefficienten müssen unabhängig von den Werthen der $\varkappa$ für sich gleich Null sein. Dasselbe gilt dann auch z. B. von $R(z_m)$; also kann man dem z_m jeden beliebigen Werth z_{m1} geben, und zu ihm Systeme $(z_{11}, z_{21}, \cdots z_{m1})$ bestimmen, welche (1) befriedigen. Wir können dies auch so auffassen, dass wir in (1) die Grösse z_m als Parameter denken und dann die Resultante $R(z_m)$ bilden. Diese ist der Annahme nach gleich 0; sonach besitzen die Gleichungen (1) für jeden Werth des Parameters z_m gemeinsame Wurzeln.

Es möge daher jetzt z_m unbestimmt bleiben. Wir setzen nun

$$(16^a)\qquad x_1 = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_{m-1} z_{m-1}$$

und führen dies statt z_{m-1} in (1) ein. Aus je $(m-1)$ der Gleichungen (1) bilden wir die Eliminante nach x_1. Dann können zwei Fälle eintreten: entweder nicht alle diese Eliminanten verschwinden identisch; oder alle diese Eliminanten verschwinden identisch. Hierdurch wird, je nachdem dieser oder jener Fall eintritt, das System (1) verschieden geartet sein.

Es sei zunächst ein $R(x_1)$ nicht identisch $= 0$, etwa das aus $f_1 = 0$, $f_2 = 0$, $\cdots f_{m-1} = 0$ gewonnene. Dann wird durch die Auflösung von $R(x_1) = 0$ jede Wurzel von (1) erhalten werden können. Die Coordinaten $(z_{11}, z_{21}, \cdots z_{m-1,1})$ treten dabei i. A. als Functionen des Parameters z_m auf; es kann aber auch vorkommen, dass $R(x_1)$ Factoren enthält, deren Coefficienten von dem Parameter z_m unabhängig sind, und dann treten neben die Lösungen erster Art

$$z_{11} = \varphi_1(z_m), \quad z_{21} = \varphi_2(z_m), \cdots z_{m-1,1} = \varphi_{m-1}(z_m); \; z_m$$

Lösungen zweiter Art, in denen alle Coordinaten feste Werthe haben.

§ 405. Ist zweitens jede der m möglichen Eliminanten $R(x_1)$ identisch Null, so ist dies auch z. B. mit jeder Eliminante $R(z_{m-1})$ der Fall; also kann man dem z_{m-1} jeden beliebigen Werth ertheilen und zu den willkürlichen z_{m-1}, z_m Systeme $(z_{11}, z_{21}, \cdots z_{m-2,1})$ bestimmen, welche (1) befriedigen. Wir betrachten jetzt z_{m-1} und z_m als Parameter und setzen

$$(16^b) \qquad x_2 = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_{m-2} z_{m-2};$$

dieses x_2 führen wir an Stelle von z_{m-2} in (1) ein. Aus je $(m-2)$ der Gleichungen (1) bilden wir die Eliminante nach x_2. Dann können zwei Fälle eintreten: entweder verschwinden nicht alle diese $\frac{1}{2} m(m-1)$ Eliminanten identisch; oder sie verschwinden sämmtlich identisch.

Es sei zunächst ein $R(x_2)$ nicht identisch $= 0$; dann wird durch die Auflösung von $R(x_2) = 0$ jede Wurzel von (1) erhalten werden können. Die Coordinaten $(z_{11}, z_{21}, \cdots z_{m-2,1})$ treten dabei i. A. als Functionen beider Parameter auf; dann werden $z_{11}, \cdots z_{m-2,1}$ Functionen von z_{m-1} und z_m. Es kann aber auch vorkommen, dass $R(x_2)$ Factoren enthält, deren Coefficienten nur von einem der beiden Parameter, etwa von z_m abhängen; dabei werden durch Vermittelung von x_2 zuerst $z_{11}, z_{21}, \cdots z_{m-2,1}$ Functionen von z_m; und weiter liefert eine beliebige der Gleichungen (1) auch $z_{m-1,1}$ als Function von z_m. Endlich ist es auch möglich, dass $R(x_2)$ Factoren besitzt, die von beiden Parametern frei sind; dabei werden $z_{11}, z_{21}, \cdots z_{m1}$ Constanten.

Die Charaktere dieser Lösungen sind also:

I) $z_{11} = \psi_1(z_{m-1}, z_m), \cdots z_{m-2,1} = \psi_{m-2}(z_{m-1}, z_m)$; z_{m-1}, z_m beliebig.

II) $z_{11} = \chi_1(z_m), \cdots z_{m-1,1} = \chi_{m-1}(z_m)$; z_m beliebig.

III) $z_{11}, z_{21}, \cdots z_{m1}$ fest. —

In solcher Weise kann man fortfahren.

Kronecker hat diese Unterscheidungen zuerst scharf durchgeführt*). Die hier benutzte Methode leitet uns sofort zu den Resultaten des allgemeinen Falles. Wir nennen mit Kronecker das System (1) ein System m^{ter} Stufe (oder m^{ten} Ranges), wenn $R(x)$ nicht identisch verschwindet, wenn also sämmtliche Wurzeln feste Coordinaten haben, oder, was das Gleiche besagt, wenn sie eine Mannigfaltigkeit 0ter Dimension bilden. — Das System (1) heisst ein System $(m-1)^{\text{ter}}$ Stufe

---

*) Grundzüge einer arithm. Theorie u. s. w. J. f. M. 91 (1881) p. 1, § 21. VII. Vgl. auch Molk, Acta math. 6 (1884) p. 1, Cap. III.

(oder $(m-1)^{\text{ten}}$ Ranges), wenn $R(x) \equiv 0$, aber ein $R(x_1)$ nicht identisch Null ist. Dann bilden die Wurzeln eine Mannigfaltigkeit erster Dimension; kommen ausser diesen keine anderen vor, so ist das System ein reines System $(m-1)^{\text{ter}}$ Stufe; kommen noch andere mit festen Coordinaten vor, dann ist das System ein solches $(m-1)^{\text{ter}}$ Stufe gemischt mit einem System m^{ter} Stufe. — Das System (1) heisst ein System $(m-2)^{\text{ter}}$ Stufe (oder $(m-2)^{\text{ten}}$ Ranges), wenn $R(x) \equiv 0$, alle $R(x_1) \equiv 0$, aber ein $R(x_2)$ nicht $\equiv 0$ ist. Dann bilden die Wurzeln eine Mannigfaltigkeit 2ter Dimension; kommen ausser diesen noch andere vor, die eine Mannigfaltigkeit erster Dimension oder solche, die eine Mannigfaltigkeit nullter Dimension bilden, dann heisst das System ein gemischtes $(m-2)^{\text{ter}}$ Stufe. — Ebenso bezeichnen wir (1) als System k^{ter} Stufe, wenn die Wurzeln eine Mannigfaltigkeit $(m-k)^{\text{ter}}$ Dimension bilden. Ist keine weitere Wurzel vorhanden, so heisst das System ein reines; treten Wurzeln auf, welche zu Mannigfaltigkeiten niederer Dimension zusammentreten, dann ist das System ein gemischtes.

Es ist nicht immer möglich, Mannigfaltigkeiten $(m-k)^{\text{ter}}$ Dimension von m Variablen durch k Gleichungen dieser Variablen rein darzustellen; also es ist etwa für $m=3$, $k=2$, um geometrisch zu sprechen, nicht möglich, durch zwei Gleichungen zwischen z_1, z_2, z_3 jede Curve dritter Ordnung rein, d. h. ohne fremde Punkte als Schnitt zweier Flächen zu bestimmen.

Neununddreissigste Vorlesung.

Elimination. Bézout'sche Methode.

§ 406. Die Darlegungen der siebenunddreissigsten Vorlesung haben uns gezeigt, dass das Problem der Elimination mancherlei Ueberlegungen und Vorbereitungen zu seiner Bewältigung bedurfte; da liegt die Frage nahe, ob nicht die stufenweise Entfernung von m Variablen $z_1, z_2, \cdots z_m$ aus den $(m+1)$ Gleichungen

(1) $\quad f_\lambda(z_1, z_2, \cdots z_m, z_{m+1}) = 0 \qquad (\lambda = 1, 2, \cdots m+1)$

rascher zum Ziele geführt hätte. Wenden wir die Methode der Elimination einer Variablen, z. B. z_1 auf die m Gleichungspaare

$$f_1 = 0,\ f_2 = 0; \quad f_1 = 0,\ f_3 = 0; \ \cdots; \ f_1 = 0,\ f_{m+1} = 0$$

an, dann erhalten wir m Gleichungen mit den m Unbekannten $z_2, z_3, \cdots z_{m+1}$. Diese Gleichungen, welche wir mit

$$g_{1,2}(z_2, \cdots z_{m+1}) = 0, \quad \cdots \quad g_{1,m+1}(z_2, \cdots z_{m+1}) = 0$$

bezeichnen, sind von den Dimensionen $n_1 n_2, n_1 n_3, \cdots n_1 n_{m+1}$, falls die Dimensionen der f wie gewöhnlich mit $n_1, n_2, \cdots n_{m+1}$ bezeichnet werden. Eliminiren wir hierauf ebenso z_2 aus den $(m-1)$ Gleichungspaaren

$$g_{1,2} = 0,\ g_{1,3} = 0; \qquad g_{1,2} = 0,\ g_{1,4} = 0; \ \cdots \ g_{1,2} = 0,\ g_{1,m+1} = 0,$$

dann ergeben sich $(m-1)$ Gleichungen in $z_3, z_4, \cdots z_{m+1}$ von den Dimensionen $n_1^2 n_2 n_3, n_1^2 n_2 n_4, \cdots n_1^2 n_2 n_{m+1}$; und fahren wir so fort, dann erlangen wir zwar eine Schluss-Eliminante, die nur z_{m+1} enthält; aber ihre Dimension

$$n_1^{2^{m-1}} \cdot n_2^{2^{m-2}} \cdots n_{m-1}^{2^1} \cdot n_m^{2^0} \cdot n_{m+1}$$

ist, wie wir bereits wissen, viel zu hoch. Wir haben nämlich bei dieser successiven Elimination zu beachten, dass die Regel über die Gradbestimmung der Eliminante sich nur auf allgemeine Gleichungen bezieht; Functionen wie $g_{1,2}, g_{1,3}, \cdots$ sind aber offenbar nicht allgemein und auch nicht unabhängig von einander. Es kann und wird demnach schon hier eine Verminderung der Dimensionszahlen eintreten. Andererseits ist es aber auch ersichtlich, dass wirklich fremde Wurzeln in die Schlussgleichung eingehen werden. Denn wenn z. B. das System vorliegt

$$f_1(z_1, z_2, z_3) = 0, \quad f_2(z_1, z_2, z_3) = 0, \quad f_3(z_1, z_2, z_3) = 0,$$
$$R_{f_1, f_2} = g_3(z_2, z_3) = 0, \quad R_{f_1, f_3} = g_2(z_2, z_3) = 0,$$
$$R_{g_3, g_2}(z_3) = 0,$$

dann wird zwar für jede Wurzel ζ_3 von $R_{g_3, g_2}(z_3) = 0$ ein Werth $z_2 = \zeta_2$ bestehen, so dass die beiden Gleichungen

$$g_3(\zeta_2, \zeta_3) = 0, \quad g_2(\zeta_2, \zeta_3) = 0$$

befriedigt sind, und ferner deswegen zwei Werte ζ_1', ζ_1'', so dass auch $f_1(\zeta_1', \zeta_2, \zeta_3) = 0$, $f_2(\zeta_1', \zeta_2, \zeta_3) = 0$ und $f_1(\zeta_1'', \zeta_2, \zeta_3) = 0$, $f_3(\zeta_1'', \zeta_2, \zeta_3) = 0$ wird; aber $(\zeta_1', \zeta_2, \zeta_3)$ ist möglicherweise keine Wurzel von $f_3 = 0$, und $(\zeta_1'', \zeta_2, \zeta_3)$ keine von $f_2 = 0$. Auch durch die Combination von f_2 und f_3 zu g_1 lässt sich dieser Uebelstand nicht beseitigen; denn es ist möglich, dass ein $(\zeta_1''', \zeta_2, \zeta_3)$ die Gleichungen $f_2 = 0$, $f_3 = 0$ befriedigt, die Gleichung $f_1 = 0$ dagegen nicht.

Wir wollen dies an einem Beispiele durchführen. Es seien die drei Gleichungen vorgelegt

$$f_1 \equiv z_1^2 - 3z_1 + z_2 + z_3 + 2 = 0,$$
$$f_2 \equiv z_1^2 + z_1 z_3 + z_2 - 1 = 0,$$
$$f_3 \equiv z_1^2 - z_1 + z_2 - z_3 - 2 = 0;$$

dann ergiebt sich bei der Resultantenbildung

$$R_{f_1,f_2} = g_{1,2}(z_2, z_3) = (z_2 + z_3)(z_3 + 3)^2,$$
$$R_{f_2,f_3} = g_{2,3}(z_2, z_3) = (z_2 - z_3 - 1)z_3(z_3 + 1),$$
$$R_{f_3,f_1} = g_{1,3}(z_2, z_3) = 4(z_2 + 2z_3 + z_3^2);$$
$$R(g_{1,3}, g_{2,3}) = h_3(z_3) = \text{cst.}\, z_3(z_3 + 1)(2z_3 + 1),$$
$$R(g_{1,2}, g_{1,3}) = h_1(z_3) = \text{cst.}\, z_3(z_3 + 1)(z_3^2 + 3z_3 + 1),$$
$$R(g_{1,2}, g_{2,3}) = h_2(z_3) = \text{cst.}\, z_3(z_3 + 1).$$

Es kommen also nur die beiden Werthe $z_3 = 0$ und $z_3 = -1$ in Frage, da diese allein alle drei Gleichungen $h_1 = 0$, $h_2 = 0$, $h_3 = 0$ befriedigen. Der erste Werth giebt aus den g als gemeinsame Wurzel von

$$9z_2 = 0, \quad 0 = 0, \quad 4z_2 = 0$$

das Resultat $z_2 = 0$. Aber für $z_2 = 0$, $z_3 = 0$ gehen die f über in

$$f_1 \equiv z_1^2 - 3z_1 + 2 = 0 \equiv (z_1 - 1)(z_1 - 2) \quad\Big|\quad f_2 \equiv z_1^2 - 1 = 0 \equiv (z_1 - 1)(z_1 + 1) \quad\Big|\quad f_3 \equiv z_1^2 - z_1 - 2 = 0 \equiv (z_1 - 2)(z_1 + 1),$$

so dass der oben als möglich hingestellte Fall hier wirklich auftritt. Dagegen liefert $z_3 = -1$ zuerst $z_2 = 1$ und dann $z_1 = 1$, und die einzige Wurzel des gegebenen Systems wird $(1, 1, -1)$.

§ 407. Unter solchen Umständen hat die Vermuthung Manches für sich, dass dieser letzte Uebelstand durch die schon früher als vortheilhaft erkannte Liouville'sche Einführung von

$$x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_{m+1} z_{m+1}$$

an Stelle von z_{m+1} sich heben lasse. In der That folgt aus dieser Transformation, wenn wir die umgewandelten Gleichungen bei $m = 2$ mit

$$g_1(z_1, z_2, x) = 0, \quad g_2(z_1, z_2, x) = 0, \quad g_3(z_1, z_2, x) = 0$$

bezeichnen,

$$R_{g_1,g_2}(x, z_2) \equiv h_1 = 0, \quad R_{g_1,g_3}(x, z_2) \equiv h_2 = 0;$$
$$R_{h_1,h_2}(x) \equiv k(x) = 0;$$

es wird also jede Wurzel von $k = 0$ direct eine gemeinsame Wurzel liefern, wenn sie gleich $\varkappa_1 z_1 + \varkappa_2 z_2 + \varkappa_3 z_3$ gesetzt werden kann. Aber hier tritt der Umstand ein, dass dies nicht bei jeder Wurzel x von $k = 0$ der Fall ist; und dadurch unterscheiden sich gerade die Wurzeln des Systems $f_1 = 0$, $f_2 = 0$, $f_3 = 0$ von den fremden Wurzeln, dass für jene die Liouville'sche Form vorhanden ist, für diese dagegen nicht. Scheiden wir alle diejenigen Factoren von $k(x) = 0$ aus, deren Wurzeln nicht in der Liouville'schen Form darstellbar sind, dann bleibt die reine Eliminantengleichung zurück.

Ein Beispiel möge auch diese Verhältnisse erläutern. Wir nehmen

$$z_1 - z_3 = 0, \quad z_2 - z_3 = 0, \quad z_1^2 - 1 = 0$$

und erhalten durch $z_3 = \varkappa_1 z_1 + \varkappa_2 z_2 + x$ die Gleichungen

$$(\varkappa_1 - 1)z_1 + \varkappa_2 z_2 + x = 0, \; \varkappa_1 z_1 + (\varkappa_2 - 1)z_2 + x = 0, \; z_1^2 - 1 = 0.$$

Durch Elimination von z_1 ergiebt sich

$$(\varkappa_2 z_2 + x)^2 - (\varkappa_1 - 1)^2 = \varkappa_2^2 z_2^2 + 2\varkappa_2 x \cdot z_2 + x^2 - (\varkappa_1 - 1)^2 = 0,$$

$$((\varkappa_2 - 1)z_2 + x)^2 - \varkappa_1^2 = (\varkappa_2 - 1)^2 z_2^2 + 2(\varkappa_2 - 1)x \cdot z_2 + x^2 - \varkappa_1^2 = 0;$$

und weiter durch Elimination von z_2 als vorläufiges Eliminationsresultat

$$x^4 - [(2\varkappa_1\varkappa_2 - \varkappa_1 - \varkappa_2 + 1)^2 + (\varkappa_1 + \varkappa_2 - 1)^2]x^2$$
$$+ [(2\varkappa_1\varkappa_2 - \varkappa_1 - \varkappa_2 + 1)(\varkappa_1 + \varkappa_2 - 1)]^2 = 0.$$

Diese Gleichung zerfällt in

$$x^2 - (\varkappa_1 + \varkappa_2 - 1)^2 = 0$$

und

$$x^2 - (2\varkappa_1\varkappa_2 - \varkappa_1 - \varkappa_2 + 1)^2 = 0,$$

deren erste die Lösungen

$$x' = \varkappa_1 + \varkappa_2 - 1; \quad x'' = -\varkappa_1 - \varkappa_2 + 1$$

und also

$$(z_1', z_2', z_3') = (-1, -1, -1), \quad (z_1'', z_2'', z_3'') = (1, 1, 1)$$

liefert, während die zweite die Wurzeln

$$x' = 2\varkappa_1\varkappa_2 - \varkappa_1 - \varkappa_2 + 1, \quad x'' = -2\varkappa_1\varkappa_2 + \varkappa_1 + \varkappa_2 - 1$$

ergiebt, von denen aus ein Uebergang zu den z_1, z_2, z_3 nicht möglich ist.

§ 408. Solche Ueberlegungen veranlassten Bézout zu dem Ausspruche, „dass man die schliessliche Eliminante wahrscheinlich nur dann frei von fremden Wurzeln erhalten würde, wenn es gelinge, alle Unbekannten mit Ausnahme einer einzigen gleichzeitig aus den vorgelegten Gleichungen zu eliminiren"*). Er war dann auch der Erste, welcher eine solche Methode veröffentlichte**) und das nach ihm benannte Theorem aufstellte und bewies. Seine Methode trägt über die sogenannten allgemeinen Gleichungen hinaus. Wir wollen ihre Grundzüge jetzt darlegen. Einige Vorbereitungen haben wir bereits in der dreissigsten Vorlesung gegeben, und eine weitere soll jetzt hergeleitet werden.

§ 409. Es seien m allgemeine vollständige Functionen von m Variablen $z_1, z_2, \cdots z_m$ gegeben

(1) $f_\alpha(z_1, z_2, \cdots z_m)$ (Dimension von f_α sei n_α; $\alpha = 1, 2, \cdots m$).

---

*) Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine p. 209, 210.

**) Théorie générale des équations algébriques. Paris 1779.

Eine weitere noch unbestimmte, allgemeine, vollständige Function derselben Variablen f_0 habe die vorläufig noch nicht näher bestimmte Dimension n_0. Wir suchen Factoren $\varphi_1, \varphi_2, \cdots \varphi_m$ auf, die gleichfalls Functionen von $z_1, z_2, \cdots z_m$ und zwar so gewählt sein sollen, dass das Aggregat

$$(2) \qquad f_0 + \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m$$

von den ersten $(m-1)$ Variablen $z_1, z_2, \cdots z_{m-1}$ frei wird und nur noch die letzte z_m enthält. Die Dimensionen von $\varphi_1, \varphi_2, \cdots \varphi_m$ nehmen wir dabei gleich $n_0 - n_1, n_0 - n_2, \cdots n_0 - n_m$, so dass alle Summanden in (2) dieselbe Dimension n_0 haben. Wir behandeln das Problem so, dass wir (2) nach seinen verschiedenen Potenzproducten von $z_1, z_2, \cdots z_{m-1}, z_m$ entwickeln und alle die Coefficienten gleich Null setzen, die zu positiven Potenzen von $z_1, z_2, \cdots z_{m-1}$ gehören. Um dabei zu verhüten, dass (2) identisch verschwindet, schreiben wir dem Coefficienten einer der Potenzen von z_m noch einen Werth $c \neq 0$ vor.

Nun hat nach § 329, (2) unser Aggregat

$$N(n_0, m) = \frac{(n_0+1)\cdots(n_0+m)}{1\cdot 2\cdots m} = \binom{n_0+m}{m}$$

Terme; von ihnen müssen alle, ausser denjenigen mit $1, z_m^1, z_m^2, \cdots z_m^{n_0}$, getilgt werden; dies giebt

$$N(n_0, m) - (n_0+1)$$

Forderungen. Endlich ist noch einem der Coefficienten, etwa dem von z_m^α, der Wert c vorgeschrieben. Es sind deshalb

$$(3) \qquad N(n_0, m) - n_0 = \binom{n_0+m}{m} - n_0$$

Bedingungen zu erfüllen.

Die Form dieser Bedingungen ist leicht zu erkennen. Wenn wir die Coefficienten der f_α mit $a_{\alpha\lambda}$, die des f_0 mit c_λ und die unbekannten Coefficienten der φ mit u_λ bezeichnen, dann sind es lineare Gleichungen von der Form

$$(4) \qquad \begin{array}{lll} a_{11}u_1 + a_{12}u_2 + \cdots + c_1 = 0 & \text{oder kürzer} & \varpi_1 + c_1 = 0, \\ a_{21}u_1 + a_{22}u_2 + \cdots + c_2 = 0 & \text{,,} \quad \text{,,} & \varpi_2 + c_2 = 0, \\ \cdots & & \cdots \end{array}$$

deren Anzahl durch (3) bestimmt ist. Wir müssen nun auch die Anzahl der verfügbaren Unbekannten u aufsuchen.

Da φ_α die Dimension $n_0 - n_\alpha$ besitzt, so ist die gesuchte Zahl

$$(3^a) \qquad \sum_\alpha N(n_0 - n_\alpha, m) \qquad (\alpha = 1, 2, \cdots m).$$

Es handelt sich nun zunächst darum, n_0 so anzunehmen, dass der

Werth von (3ᵃ) demjenigen von (3) mindestens gleichkommt. Diese Aufgabe ist durch die Formel (11ᵃ), § 333 bereits gelöst; sie lautet

$$\sum_{\lambda=1}^{k} N(n-a_\lambda, k) > N(n, k) - a_1 \cdot a_2 \cdots a_k, \quad \left(\sum a_\lambda \leq n+k\right).$$

Setzt man also $n_0 = n_1 \cdot n_1 \cdots n_m$, dann ist

$$(5) \qquad \sum_{\alpha} N(n_1 \cdot n_2 \cdots n_m - n_\alpha, m) > N(n_1 \cdot n_2 \cdots n_m, m) - n_1 \cdot n_2 \cdots n_m.$$

Es reicht daher aus, wenn als Dimension von f_0 das Product aller Dimensionen der $f_1, f_2, \cdots f_m$ genommen wird.

§ 410. Dadurch, dass in (4) die Anzahl der Unbekannten u diejenige der Gleichungen übertrifft, ist aber die Lösbarkeit der Aufgabe noch nicht verbürgt. Denn es wäre möglich, dass die linken Seiten der Gleichungen (4) nicht von einander unabhängig sind, und es wäre weiter möglich, dass die von einander unabhängigen Gleichungen (4) sich widersprechen. Sobald aber für eine besondere Annahme der Functionen $f_1, f_2, \cdots f_m$ bei unbestimmten c_λ eine Lösung nachgewiesen ist, können wir den Schluss ziehen, dass auch im allgemeinen Falle eine Lösung besteht.

Im allgemeinen Falle ist nämlich die Lösung dann und nur dann unmöglich, wenn bei unbestimmten c_λ eine Gleichung

$$(6) \qquad \varkappa_1 \varpi_1 + \varkappa_2 \varpi_2 + \cdots + \varkappa_\varrho \varpi_\varrho = 0$$

besteht, in der die $\varkappa$ von den Variablen frei sind. Die $\varkappa$ sind auf mancherlei Art als Subdeterminanten des zu $\varpi_1, \varpi_2, \cdots$ gehörigen Coefficientensystems frei von den c_λ darstellbar. Diese können bei besonderen Werthen der $a_{\varkappa\lambda}$ sämmtlich verschwinden; das ist dann ein Zeichen dafür, dass schon zwischen einer geringeren Anzahl von ϖ Relationen bestehen. Bleiben die c unbestimmt, so ist dieser besondere, wie jener allgemeinere Fall von Relationen ausgeschlossen, sobald die Gleichungen für specielle Annahme der f lösbar sind. Sind dagegen die c gegeben, so könnte wohl die allgemeinere Relation (6) den gegebenen Werthen der c widersprechen, während die besonderen neuen Relationen keinen Widerspruch finden würden. Darin liegt der Grund, bei den beweisenden Beispielen die c unbestimmt zu lassen.

Wir wollen das Besprochene an einem Beispiele erläutern. Es sei das System gegeben

$$\begin{aligned}
\varpi_1 &\equiv (1+\alpha)z_1 + (1+3\alpha)z_2 + (1-\alpha)z_3 = 2,\\
\varpi_2 &\equiv (1-\alpha)z_1 + (1+2\alpha)z_2 + (1-4\alpha)z_3 = 2,\\
\varpi_3 &\equiv \qquad\qquad\qquad\quad z_2 \qquad - \qquad z_3 = 1;
\end{aligned}$$

hier besteht zwischen den drei ϖ die Relation

(7) $$(1-\alpha)\varpi_1 - (1+\alpha)\varpi_2 + (\alpha + 5\alpha^2)\varpi_3 = 0;$$

da aber im Allgemeinen, d. h. für unbestimmte α,

$$(1-\alpha)\cdot 2 - (1+\alpha)\cdot 2 + (\alpha+5\alpha^2)\cdot 1 \neq 0$$

wird, so ist im Allgemeinen das System der obigen drei Gleichungen nicht lösbar. Benutzen wir aber gerade die Beziehung

$$(1-\alpha)\cdot 2 - (1+\alpha)\cdot 2 + (\alpha+5\alpha^2)\cdot 1 = 0$$

zur Bestimmung von α, so folgt, dass für $\alpha = 0$ und für $\alpha = \frac{3}{5}$ die Relation (7) identisch befriedigt ist; allein an ihre Stelle tritt für

$$\alpha = \frac{3}{5} \quad \text{die Relation} \quad \varpi_1 - 4\varpi_2 + 30\varpi_3 = 0,$$

und also ist das besondere System auch jetzt nicht lösbar; und für

$$\alpha = 0 \quad \text{die Relation} \quad \varpi_1 - \varpi_2 = 0,$$

so dass dieses besondere System eine Lösung hat, obwohl das allgemeine nicht lösbar ist. Auf diese Verhältnisse hat Herr C. Schmidt: „Zur Theorie der Elimination“, Schlöm. Zeitschr. 31 (1886), p. 214 zuerst aufmerksam gemacht.

Um die allgemeine Lösbarkeit des Systems (4) nachzuweisen, reicht es somit aus, sie für irgend eine besondere Wahl der f bei unbestimmt gelassenen c_λ darzulegen.

§ 411. Um ein solches Beispiel zu liefern, setzen wir*)

$$f_1 = z_1^{n_1} - a, \quad f_2 = z_2^{n_2} - z_1, \quad f_3 = z_3^{n_3} - z_2, \quad \cdots$$
$$f_{m-1} = z_{m-1}^{n_{m-1}} - z_{m-2} \quad f_m = z_m^{n_m} - z_{m-1}.$$

Diese Functionen verwenden wir zur Reduction einer allgemeinen Function f_0 von der Dimension $(n_1 \cdot n_2 \cdots n_m)$ mit unbestimmten Coefficienten. Zunächst dividiren wir f_0 durch f_m, bis ein Rest $f_0^{(1)}$ bleibt, der in z_m nicht bis zum Grade n_m aufsteigt. Der Quotient steigt bis zur Dimension $(n_1 \cdot n_2 \cdots n_m) - n_m$ auf; wir nennen ihn $-\psi_m$ und haben

$$f_0 + \psi_m f_m = f_0^{(1)}.$$

Die Dimension von $f_0^{(1)}$ ist nicht grösser als $(n_1 \cdots n_m)$. Wir dividiren $f_0^{(1)}$ durch f_{m-1}, bis ein Rest $f_0^{(2)}$ bleibt, der in z_{m-1} nicht bis zum Grade n_{m-1} aufsteigt. Den Quotienten, dessen Dimension $(n_1 \cdots n_m) - n_{m-1}$ nicht übertrifft, nennen wir $-\psi_{m-1}$ und haben

$$f_0 + \psi_{m-1} f_{m-1} + \psi_m f_m = f_0^{(2)}.$$

---

*) C. Schmidt, l. c., p. 218 macht die Ueberlegungen in der angeführten Weise am oben benutzten Beispiele.

Da die letzte Division einzeln in allen nach z_m geordneten Gliedern ausgeführt werden kann, so ist in dem Grade nach z_m keine Aenderung eingetreten, und $f_0^{(2)}$ steigt in z_{m-1} und z_m höchstens bis zu den Graden n_{m-1} bezw. n_m. Fährt man weiter so fort, dann gelangt man zu dem ersten Resultate:

$$(8)\quad f_0 + \psi_1 f_1 + \psi_2 f_2 + \cdots + \psi_m f_m = \sum d_h \cdot z_1^{h_1} z_2^{h_2} \cdots z_m^{h_m} \quad (h_\alpha < n_\alpha).$$

Nach diesen vorbereitenden Vereinfachungen reicht es also aus, das allgemeine Glied $z_1^{h_1} z_2^{h_2} \cdots z_m^{h_m}$ zu behandeln, in welchem jedes $h_\alpha < n_\alpha$ zu nehmen ist, sonst aber einen beliebigen positiven Werth haben kann.

Aus der Form von f_2 folgt

$$f_2 \cdot [z_2^{n_2(h_1-1)} + z_2^{n_2(h_1-2)} z_1 + \cdots + z_2^{n_2} \cdot z_1^{h_1-2} + z_1^{h_1-1}] = z_2^{n_2 h_1} - z_1^{h_1},$$

so dass wir in dem zu reducirenden Gliede

$$z_1^{h_1} = z_2^{h_1 n_2} - f_2 \cdot [z_2^{n_2(h_1-1)} + \cdots + z_1^{h_1-1}]$$

setzen können. Dies geht dadurch in die Form

$$(9)\qquad z_2^{h_1 n_2 + h_2} z_3^{h_3} \cdots z_m^{h_m} + f_2 \cdot T_2$$

über, wobei T_2 als Dimension besitzt

$$\begin{aligned} n_2(h_1-1) + h_2 + \cdots + h_m &< -n_2 + h_1 n_2 n_3 \cdots n_m + h_2 n_3 n_4 \cdots n_m + \cdots \\ &< -n_2 + (n_1-1) n_2 n_3 \cdots n_m + (n_2-1) n_3 n_4 \cdots n_m + \cdots \\ &< (n_1 n_2 \cdots n_m) - n_2 . \end{aligned}$$

Tragen wir also die Reduction (9) in (8) ein, dann können wir links $(\psi_2 - T_2)$ statt ψ_2 schreiben, ohne die Dimensionsvorschriften zu verletzen. Jetzt setzen wir ähnlich auf Grund der Form von f_3

$$z_2^{h_1 n_2 + h_2} = z_3^{h_1 n_2 n_3 + h_2 n_3} - f_3 \cdot [z_3^{n_3(h_1 n_2 + h_2 - 1)} + \cdots + z_2^{h_1 n_2 + h_2 - 1}],$$

tragen dies in (9) ein und erhalten statt $z_1^{h_1} z_2^{h_2} \cdots z_m^{h_m}$ die Form

$$(10)\qquad z_3^{h_1 n_2 n_3 + h_2 n_3 + h_3} \cdot z_4^{h_4} \cdots z_m^{h_m} + f_2 T_2 + f_3 T_3 .$$

Dabei besitzt T_3 als Dimension

$$\begin{aligned} & n_3(h_1 n_2 + h_2 - 1) + h_3 + \cdots + h_m \\ &< -n_3 + h_1 n_2 n_3 \cdots n_m + h_2 n_3 n_4 \cdots n_m + h_3 n_4 \cdots n_m + \cdots \\ &< -n_3 + (n_1-1) n_2 n_3 \cdots n_m + (n_2-1) n_3 n_4 \cdots n_m + (n_3-1) n_4 \cdots n_m + \cdots \\ &< (n_1 n_2 \cdots n_m) - n_3 . \end{aligned}$$

Also auch jetzt können wir, da die Dimension gewahrt bleibt, bei der Eintragung in (8) das T_3 zu dem ψ_3 ziehen. So gelangt man schliesslich zu der geforderten Reduction und Elimination

$$z_m^{h_1 n_2 n_3 \cdots n_m + h_2 n_3 \cdots n_m + \cdots + h_m} + f_2 T_2 + f_3 T_3 + \cdots + f_m T_m .$$

Der Exponent von z_m erreicht höchstens den Werth $(n_1 n_2 \cdots n_m) - 1$, so dass also wirklich die Reduction abgeschlossen ist.

§ 412. Wir können nunmehr den Satz aussprechen: Sind

(1) $f_\alpha(z_1, z_2, \cdots z_m)$ (Dimension von f_α ist n_α; $\alpha = 1, 2, \cdots m$)

allgemeine Functionen der m Veränderlichen z, dann lassen sich eben so viele Factoren

$$\varphi_\alpha(z_1, z_2, \cdots z_m) \text{ der Dimension } (n_1 n_2 \cdots n_m) - n_\alpha$$

derart herstellen, dass wenn f_0 eine allgemeine Function der z von der Dimension $(n_1 n_1 \cdots n_m)$ bezeichnet, das Aggregat

$$(2) \qquad f_0 + \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m$$

eine Function von z_m allein wird. Setzt man jetzt, was ja erlaubt ist, alle Coefficienten von f_0 gleich Null, während die $f_1, \cdots f_m$ allgemeine Functionen bleiben, dann folgt: Bedeuten die f_α in (1) allgemeine Functionen, dann kann man die φ_α so bestimmen, dass

$$(11) \qquad \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m = G(z_m)$$

d. h. eine Function von z_m allein wird, deren Dimension das Product der Dimensionen der $f_1, f_2, \cdots f_m$ nicht übersteigt. Geht man endlich von (11) zu speciellen Functionen f_α und bedenkt, dass dafür gesorgt ist, dass G nicht identisch verschwinde, dann folgt: Auch für beliebig vorgelegte besondere Functionen f_α gilt der letzte Satz.

§ 413. Wir wollen nun annehmen, es wäre möglich, auf zwei verschiedene Arten solche Eliminanten

$$(11) \qquad \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m = G(z_m),$$
$$(12) \qquad \psi_1 f_1 + \psi_2 f_2 + \cdots + \psi_m f_m = H(z_m)$$

herzustellen, wobei aber über die Dimensionen der $\varphi_1, \cdots \varphi_m$; $\psi_1, \cdots \psi_m$; G, H nichts vorausgesetzt werden soll. Angenommen, der Grad von G ist nicht kleiner als der von H, dann kann man durch Division

$$G(z_m) = H(z_m) \cdot Q(z_m) + K(z_m), \qquad [K] < [H]$$

erlangen und demgemäss aus (11) und (12)

$$(13) \quad (\varphi_1 - Q \cdot \psi_1) f_1 + (\varphi_2 - Q \cdot \psi_2) f_2 + \cdots + (\varphi_m - Q \cdot \psi_m) f_m = K(z_m)$$

herleiten. Gesetzt nun, H sei die niedrigste nicht verschwindende Function, welche einer solchen Gleichung wie (11) genügt, dann zeigt (13), dass K identisch verschwinden muss, d. h.: Alle Functionen $G(z_m)$, die sich in der Form (11) aus $f_1, f_2, \cdots$ herleiten lassen, sind Multipla einer gewissen Function niedrigsten Grades H. Ist nun etwa $G = H \cdot Q$, so tritt an die Stelle von (13)

$$(13^a) \quad (\varphi_1 - Q\psi_1) f_1 + (\varphi_2 - Q\psi_2) f_2 + \cdots + (\varphi_m - Q\psi_m) f_m = 0.$$

Diese Gleichung kann nun entweder so erfüllt sein, dass jede der Klammern gleich Null ist, $\varphi_\alpha = Q\psi_\alpha$ für jedes α, oder dass eine Beziehung

$$(14) \qquad \chi_1 \cdot f_1 + \chi_2 \cdot f_2 + \cdots + \chi_m \cdot f_m = 0$$

mit nicht verschwindenden Coefficienten χ besteht. Nur wenn eine Relation (14) besteht, ist es möglich, eine Function $G(z_m)$ auf mehrfache Weise in der Form (11) darzustellen. Von der Existenz solcher Relationen überzeugt man sich leicht; es reicht z. B. aus, $\chi_1 = f_2$, $\chi_2 = -f_1$ und alle anderen $\chi = 0$ zu wählen. Auf die allgemeine Herleitung derselben gehen wir später ein.

Wir können jetzt beweisen: Bei allgemeinen Functionen $f_\alpha(z_1, \cdots z_m)$ giebt es kein $G(z_m)$ von geringerem als dem $(n_1 \cdot n_2 \cdots n_m)^{\text{ten}}$ Grade, so dass bis auf einen constanten Factor $G(z_m)$ eindeutig bestimmt ist. $G(z_m)$ ist irreductibel. Gäbe es nämlich ein $H(z_m)$ von geringerem, so sei es zugleich von möglichst niedrigem Grade; dann wäre G ein Vielfaches von H. Es reicht also aus, an einem Beispiele nachzuweisen, dass G für einen besonderen Fall nicht zerlegbar ist und den angegebenen Grad hat, dann ergeben sich die obigen Sätze daraus ohne Weiteres. Unser voriges Beispiel ist auch für diesen Zweck ausreichend. Wir setzen

$$f_1 = z_1^{n_1} - a, \quad \varphi_1 = 1,$$
$$f_2 = z_2^{n_2} - z_1, \quad \varphi_2 = z_2^{n_2(n_1-1)} + z_2^{n_2(n_1-2)} z_1 + \cdots + z_1^{n_1-1},$$
$$f_3 = z_3^{n_3} - z_2, \quad \varphi_3 = z_3^{n_3(n_2 n_1-1)} + z_3^{n_3(n_2 n_1-2)} z_2 + \cdots + z_2^{n_2 n_1-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_1\varphi_1 = z_1^{n_1} - a; \quad f_2\varphi_2 = z_2^{n_2 n_1} - z_1^{n_1}, \quad f_3\varphi_3 = z_3^{n_3 n_2 n_1} - z_2^{n_2 n_1}, \cdots$$
$$\varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m = z_m^{n_1 n_2 \cdots n_m} - a.$$

Dieser Ausdruck hat den vorgeschriebenen Grad und ist für ein allgemeines a irreductibel, weil er in a linear ist.

Es möge hier nochmals hervorgehoben werden, dass zwar $G(z_m)$ bestimmt ist, dass aber die φ verschiedentlich gewählt werden können.

§ 414. Die in § 412, (11) gefundene Function lässt sich noch von anderen Gesichtspunkten aus betrachten. Sind die Gleichungen (1) vorgelegt, und bedeuten

$$(z_{11}, z_{21}, \cdots z_{m1}), \quad (z_{12}, z_{22}, \cdots z_{m2}), \cdots (z_{1k}, z_{2k}, \cdots z_{mk})$$

ihre gemeinsamen Wurzelsysteme, dann wird gemäss (11) die Function $G(z_m)$ für jeden der Werthe $z_{m,1}, z_{m,2}, \cdots z_{m,k}$ den Werth Null annehmen. G verschwindet also zugleich mit allen f_α, und es kann $G = 0$ deshalb als eine Folge der Gleichungen (1) angesehen werden. Jedenfalls kommt daher das Product

$$(z_m - z_{m1})(z_m - z_{m2}) \cdots (z_m - z_{mk})$$

als Factor von $G(z_m)$ vor. Nach der Theorie der symmetrischen Functionen mehrerer Variablenreihen ist dieses Product durch die Coefficienten der f_α rational darstellbar. Es müsste also G, wenn es nicht jenem Producte bis auf einen von z_m unabhängigen Factor gleich ist, zerfallen. Das ist nach den Ergebnissen des vorigen Paragraphen nicht möglich. Folglich ist

$$G(z_m) = \text{cst.}\,(z_m - z_{m1})(z_m - z_{m2}) \cdots (z_m - z_{mk}), \quad k = n_1 n_2 \cdots n_m.$$

Damit ist die Uebereinstimmung von $G(z_m)$ mit der Eliminante $R(z_m)$ nachgewiesen. Es ist aber wohl zu beachten, dass wir bei der Benutzung des Satzes aus der Theorie der symmetrischen Functionen schon die Kenntniss eines grossen Theils der früher abgeleiteten Resultanteneigenschaften vorausgesetzt haben. Es ist deshalb sehr wünschenswerth, die Bézout'sche Theorie durch den Nachweis des letzten Satzes unabhängig von Früherem vollständig zu machen, indem wir zeigen, dass zu jeder Wurzel $z_{m\alpha}$ von $G(z_m) = 0$ Coordinaten $z_{1\alpha}, z_{2\alpha}, \cdots z_{m-1,\alpha}$ gefunden werden können, so dass $(z_{1\alpha}, z_{2\alpha}, \cdots z_{m\alpha})$ eine Wurzel von (1) ist.

Bézout hat die Nothwendigkeit dieses Nachweises nicht bemerkt; auch Liouville hat sie übersehen; Serret*) giebt einen Beweis, der freilich den Satz versteckter Weise schon als richtig voraussetzt. Herr C. Schmidt hat (l. c.) einen Beweis geliefert, den wir mit einigen nothwendig erscheinenden Änderungen folgen lassen wollen.

§ 415. Wir setzen als Liouville'sche Substitution an

$$(15) \qquad x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_{m-1} z_{m-1} + z_m,$$

in welcher wir der Einfachheit halber den Coefficienten von z_m gleich 1 nehmen; in alle f_α tragen wir $z_m = x - \varkappa_1 z_1 - \cdots$ ein und erhalten dadurch die Umwandlung

$$f_\alpha(z_1, z_2, \cdots z_m) = g_\alpha(z_1, \cdots z_{m-1}; x) \qquad (\alpha = 1, 2, \cdots m).$$

Das Bézout'sche Verfahren liefert dann bei der Elimination von $z_1, z_2, \cdots z_{m-1}$ eine Gleichung von der Form

$$\sum_\alpha \psi_\alpha(z_1, \cdots z_{m-1}; x) g_\alpha(z_1, \cdots z_{m-1}; x) = H(x) \quad (\alpha = 1, 2, \cdots m).$$

Trägt man hier umgekehrt (15) ein, so gehen die g_α wieder in die f_α über, die von $\varkappa_1, \varkappa_2, \cdots \varkappa_{m-1}$ frei sind,

$$(16) \quad \sum_\alpha \chi_\alpha(z_1, \cdots z_m; \varkappa_1, \cdots) f_\alpha(z_1, \cdots z_m) = H(\varkappa_1 z_1 + \cdots + \varkappa_{m-1} z_{m-1} + z_m; \varkappa_1, \cdots).$$

*) Cours d'algèbre supérieure; 3. Aufl. Paris 1866. Bd. 1, p. 162.

Nun entwickeln wir nach den $\varkappa$ zuerst

$$\chi_\alpha = \varphi_\alpha + (\varphi_{\alpha 1} \cdot \varkappa_1 + \cdots + \varphi_{\alpha m-1} \cdot \varkappa_{m-1}) + \cdots \quad (\alpha = 1, 2, \cdots m).$$

$$H(x; \varkappa_1, \cdots) = H_0(x) + [H_1(x) \cdot \varkappa_1 + \cdots + H_{m-1}(x) \cdot \varkappa_{m-1}] + \cdots$$

und dann weiter

$$H_\alpha(x) = H_\alpha(z_m) + H'_\alpha(z_m)[z_1 \cdot \varkappa_1 + \cdots + z_{m-1} \cdot \varkappa_{m-1}] + \cdots$$

Tragen wir dies Alles in (16) ein und vergleichen die Coefficienten von $\varkappa_1, \varkappa_2, \cdots \varkappa_{m-1}$ und die von den $\varkappa$ unabhängigen Glieder, bedenken dabei aber zugleich, dass für $\varkappa_1 = \varkappa_2 = \cdots = \varkappa_{m-1} = 0$ das x zu z_m und also $H_0(x)$ zu $G(z_m)$ wird, so entsteht

$$(17) \quad \begin{aligned} \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m &= G(z_m), \\ \varphi_{11} f_1 + \varphi_{12} f_2 + \cdots + \varphi_{1m} f_m &= z_1 G'(z_m) + H_1(z_m), \\ \varphi_{21} f_1 + \varphi_{22} f_2 + \cdots + \varphi_{2m} f_m &= z_2 G'(z_m) + H_2(z_m), \\ \cdots\cdots & \cdots\cdots \\ \varphi_{m-1,1} f_1 + \cdots + \varphi_{m-1,m} f_m &= z_{m-1} G'(z_m) + H_{m-1}(z_m). \end{aligned}$$

Bezeichnen wir die Determinante der φ auf der linken Seite von (17) mit Δ, so folgt, dass die m Producte

$$\Delta f_1, \quad \Delta f_2, \cdots \Delta f_m$$

lineare ganze Functionen der m Ausdrücke

$$G(z_m), \quad z_1 G'(z_m) + H_1(z_m), \cdots z_{m-1} G'(z_m) + H_{m-1}(z_m)$$

sind. Wenn also z_{m1} als Wurzel von $G(z_m) = 0$ genommen und

$$z_{11} = -\frac{H_1(z_{m1})}{G'(z_{m1})}, \cdots \quad z_{m-1,1} = -\frac{H_{m-1}(z_{m1})}{G'(z_{m1})}$$

gesetzt wird, so ist das System (1) befriedigt, falls durch diese Substitutionen Δ einen von Null verschiedenen Werth annimmt. Zu beachten ist, dass $G(z_m)$ irreductibel ist (§ 413), also $G'(z_{m1}) \neq 0$ wird.

Wir haben demnach zu beweisen, dass Δ durch die Substitutionen

$$(18) \quad z_1 = -\frac{H_1(z_m)}{G'(z_m)}, \cdots z_{m-1} = -\frac{H_{m-1}(z_m)}{G'(z_m)}$$

einen Werth annimmt, der durch $G(z_m)$ nicht theilbar ist.

Sollte eine solche Theilbarkeit bei allgemeinen Functionen vorhanden sein, so müsste sie auch bei jedem besonderen Systeme erhalten bleiben. Besteht sie also in einem speciellen Falle nicht, dann sind wir sicher, dass sie auch bei allgemeinen Functionen nicht vorhanden ist. Wir werden nun ein Beispiel liefern, bei welchem die Theilbarkeit nicht vorhanden ist.

§ 416. Es sei

$$f_1 = z_1^{n_1} - 1, \quad f_2 = z_2^{n_2} - z_1, \quad f_3 = z_3^{n_3} - z_2, \cdots f_m = z_m^{n_m} - z_{m-1}.$$

Wir untersuchen zunächst, welche Form eine identische Gleichung

$$A_1 f_1 + A_2 f_2 + \cdots + A_m f_m \equiv 0$$

haben muss, in welcher die A ganze Functionen von $z_1, z_2, \cdots z_m$ bedeuten. Setzen wir z. B. $f_1 = 0$, $f_2 = 0$; $f_4 = 0$, $f_5 = 0, \cdots f_m = 0$, so muss, weil dabei z_3 ganz beliebig gewählt werden kann, A_3 identisch Null werden. In A_3 substituiren wir der Reihe nach

$$z_1 = z_2^{n_2} - f_2; \quad z_4 = z_5^{n_5} - f_5, \quad z_5 = z_6^{n_6} - f_6, \cdots z_{m-1} = z_m^{n_m} - f_m,$$

dann entsteht

$$A_3 = B_3(z_2; z_3, z_m) + b_2 \cdot f_2 + b_5 \cdot f_5 + b_6 \cdot f_6 + \cdots + b_m \cdot f_m;$$

ferner dividiren wir B_3 durch $z_2^{n_1 n_2} - 1 = f_1 + c_2 \cdot f_2$ und den Rest sowie die Coefficienten des Quotienten durch

$$z_m^{n_1 n_2 \cdots n_m} - z_3 = f_4 + c_5 f_5 + c_6 f_6 + \cdots + c_m f_m.$$

Hier sind die b und die c Functionen der z. So entsteht

$$A_3 = D_3(z_2; z_3, z_m) + d_{31} \cdot f_1 + d_{32} \cdot f_2 + d_{34} \cdot f_4 + \cdots + d_{3,m} \cdot f_m;$$

D_3 steigt in z_2 nur bis zur $(n_1 n_2 - 1)^{\text{ten}}$ Potenz und in z_m nur bis zur $(n_1 n_2 \cdots n_m - 1)^{\text{ten}}$ Potenz. Wir untersuchen jetzt

$$D_3 = e_0 + e_1 \cdot z_2 + e_2 \cdot z_2^2 + \cdots + e_{n_1 n_2 - 1} z_2^{n_1 n_2 - 1},$$

wobei die e nur noch z_3 und z_m enthalten. Nehmen wir für z_m eine Wurzel der Gleichung

$$z_m^{n_1 n_2 \cdots n_m} - z_3 = 0, \tag{19}$$

so können wir einerseits $z_4, z_5, \cdots z_{m-1}$ so bestimmen, dass $f_4 = 0, \cdots f_m = 0$ wird; und wenn dann andrerseits für z_2 alle Wurzeln von

$$z_2^{n_1 n_2} - 1 = 0$$

gewählt werden, so kann man zu jeder ein z_1 so bestimmen, dass $f_1 = 0$, $f_2 = 0$ wird. Folglich muss für jeden dieser $n_1 n_2$ Werthe von z_2 auch $D_3 = 0$ sein. Das geht nur so, dass jedes $e_0, e_1, \cdots$ Null ist. Da aber die e nur bis zum Grade $(n_1 n_2 \cdots n_{m-1})$ aufsteigen, während z_m gemäss (19) $n_1 n_2 \cdots n_m$ verschiedene Werthe annehmen kann, so sind alle e identisch Null, und es wird

$$A_3 = d_{31} f_1 + d_{32} f_2 + d_{34} f_4 + \cdots + d_{3m} f_m. \tag{20}$$

Die entsprechenden Resultate gelten für alle $A_1, A_2, \cdots A_m$. —

Wir bilden jetzt mit den Functionen f das $H(x)$. Diese Function steigt bis zum Grade $k = n_1 n_2 \cdots n_m$; wir kennen die k Wurzeln von $H(x) = 0$, nämlich, wenn ω eine primitive k^{te} Einheitswurzel bedeutet,

$$x_\lambda = \omega^\lambda + \varkappa_{m-1} \omega^{\lambda n_m} + \varkappa_{m-2} \omega^{\lambda n_{m-1} n_m} + \cdots \quad (\lambda = 1, 2, \cdots k);$$

also ist

$$H(x) = \Pi(x - x_\lambda) = \Pi[(z_m - \omega^\lambda) + \varkappa_{m-1}(z_{m-1} - \omega_m^{\lambda n_m}) + \cdots]$$

$$= (z_m^k - 1) + \varkappa_{m-1}(z_m^k - 1) \sum \frac{z_{m-1} - \omega^{\lambda n_m}}{z_m - \omega^\lambda} + \cdots$$

$$= (z_m^k - 1) + \varkappa_{m-1}[k z_{m-1} \cdot z_m^{k-1} - k z_m^{n_m - 1}]$$

$$+ \varkappa_{m-2}[k z_{m-2} \cdot z_m^{k-1} - k z_m^{n_{m-1} n_m - 1}] + \cdots .$$

Die Richtigkeit der durchgeführten Summationen ist durch Zerlegung in Partialbrüche leicht zu erkennen. Man hat also

$$G(z_m) = z_m^k - 1,$$

$$z_1 G'(z_m) + H_1(z_m) = k(z_1 \cdot z_m^{k-1} - z_m^{n_2 \cdots n_m - 1}),$$

$$z_2 G'(z_m) + H_2(z_m) = k(z_2 \cdot z_m^{k-1} - z_m^{n_3 \cdots n_m - 1}),$$

$$\cdots\cdots\cdots\cdots$$

$$z_{m-1} G'(z_m) + H_{m-1}(z_m) = k(z_{m-1} \cdot z_m^{k-1} - z_m^{n_m - 1}).$$

Damit ist der erste Theil der Aufgabe gelöst, indem die rechten Seiten der Gleichungen (17) gefunden sind. Wir müssen jetzt zweitens die gefundenen Functionen in die Form der linken Seiten von (17) bringen. Dazu setzen wir

$$(21) \qquad z_m^k - 1 = f_1 + t_2 f_2 + t_3 f_3 + \cdots + t_m f_m ;$$

ferner ergiebt sich leicht für passende t und τ

$$(21^a) \quad \begin{aligned} k(z_1 \cdot z_m^{k-1} - z_m^{n_2 n_3 \cdots - 1}) &= k z_m^{k-1} f_2 + t_{13} f_3 + \cdots + t_{1m} f_m + \tau_1 \cdot (z_m^k - 1), \\ k(z_2 \cdot z_m^{k-1} - z_m^{n_3 n_4 \cdots - 1}) &= \qquad k z_m^{k-1} f_3 + \cdots + t_{2m} f_m + \tau_2 \cdot (z_m^k - 1), \\ &\cdots\cdots\cdots\cdots \\ k(z_{m-1} \cdot z_m^{k-1} - z_m^{n_m - 1}) &= \qquad\qquad k z_m^{k-1} f_m + \tau_{m-1} (z_m^k - 1). \end{aligned}$$

Formen wir in diesen letzten $(m-1)$ Gleichungen je das letzte Glied der rechten Seite mit Hülfe der Darstellung (21) von $(z_m^k - 1)$ um, dann sind die Ausdrücke sämmtlich in die vorgeschriebene Form gebracht. Bei der Bildung der Determinante Δ spielt diese Umformung aber keine Rolle, denn wir können ja, ohne Δ zu ändern, von den letzten $(m-1)$ Zeilen die Elemente der Zeile (21), mit $\tau_1, \tau_2, \cdots \tau_{m-1}$ multiplicirt abziehen. So erhält man als Resultat $(k z_m^{k-1})^{m-1}$. Das ist aber möglicherweise noch nicht der geforderte Ausdruck, denn die Darstellung (21) ist nicht eindeutig. Nach dem ersten Resultate dieses Paragraphen könnte noch zu jeder Zeile rechts ein Ausdruck

$$A_1 f_1 + A_2 f_2 + \cdots + A_m f_m = 0$$

hinzukommen. Die Aenderung der Elemente der Determinante würde also nur darin bestehen, dass Ausdrücke der Form (20) hinzutreten. Folglich ist

$$\Delta = (kz_m^{k-1})^{m-1} + g_1 f_1 + g_2 f_2 + \cdots + g_m f_m.$$

Jetzt können wir entscheiden, ob Δ unter den Annahmen (18) durch $G(z_m)$ theilbar wird, oder, was dasselbe sagt, ob Δ für

$$z_m = \omega, \quad z_{m-1} = \omega^{n_m}, \quad z_{m-2} = \omega^{n_{m-1} n_m}, \cdots$$

gleich Null ist. Durch diese Werthe erhält man $f_1 = 0$, $f_2 = 0, \cdots f_m = 0$ und somit

$$\Delta = k^{m-1} \omega^{-m+1}.$$

Es ist demnach Δ von Null verschieden. Damit ist der Beweis erbracht. Die Bézout'sche Methode liefert

$$(11^a) \qquad \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m = R(z_m),$$

wobei $R(z_m)$ die Eliminante der Functionen f_α bedeutet.

§ 417. Die Functionen f_α sind bisher als allgemeine, vollständige Functionen vorausgesetzt worden. Ist unter dieser Annahme (11^a) gebildet, so reicht es bei besonderen, gegebenen f_α aus, die allgemeinen Coefficienten durch die besonderen zu ersetzen, um auch in diesem Falle die Eliminante in der Form (11^a) darzustellen. Natürlich kann es dabei vorkommen, dass der Grad von $R(z_m)$ sich vermindert, oder auch dass R direct identisch gleich Null wird. —

Sind die f_α allgemeine Functionen, so wollen wir sie sowie die φ_α nach absteigenden Dimensionen der Potenzproducte ordnen,

$$f_\alpha = g_\alpha + g'_\alpha + g''_\alpha + \cdots, \quad \varphi_\alpha = \psi_\alpha + \psi'_\alpha + \psi''_\alpha + \cdots,$$

wobei also g_α alle Glieder enthält, die von der Dimension n_α sind, und ψ_α alle von der Dimension $(k - n_\alpha)$. Trägt man dies in (11^a) ein, dann folgt, dass $\Sigma g_\alpha \psi_\alpha$ die Glieder der höchsten vorkommenden Dimension k umfasst. Folglich ist diese Summe gleich dem Gliede höchsten Grades in

$$G(z_m) = R(z_m) = \varrho_0 z_m^k + \varrho_1 z_m^{k-1} + \cdots,$$

d. h. man hat die Gleichung

$$\psi_1 g_1 + \psi_2 g_2 + \cdots + \psi_m g_m = \varrho_0 z_m^k,$$

worin ϱ_0 frei von den Variablen ist. Dies zeigt uns: Sind in (11^a) die Functionen f_α homogen von den Dimensionen n_α, dann wird die rechte Seite $= \varrho_0 z_m^k$, wobei ϱ_0 eine Function der Constanten allein ist. —

Von diesem Satze aus können wir nun auch zur Darstellung der Resultanten für $(m + 1)$ Gleichungen $f_\alpha = 0$ $(\alpha = 1, 2, \cdots m + 1)$ mit den m Unbekannten $z_1, z_2, \cdots z_m$ gelangen.

Zu diesem Zwecke reicht es aus, in die f_α eine neue Variable t einzuführen, durch welche unter Wahrung der Dimensionen n_α jede der Functionen homogen wird. Für das neue System von $(m+1)$ Gleichungen mit ebenso vielen Unbekannten bilden wir nach der Bézout'schen Methode die Eliminante für t. So entsteht in Gemässheit unseres letzten Resultates

$$(11^b) \qquad \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_{m+1} f_{m+1} = \varrho_0 t^l,$$

wobei ϱ_0 von den Unbekannten frei ist. Denken wir nun t wieder durch 1 ersetzt, dann zeigt sich, dass die $f_\alpha = 0$ nur dann eine gemeinsame Wurzel haben, wenn $\varrho_0 = 0$ ist. Wenn umgekehrt $\varrho_0 = 0$ ist, so wird die Eliminante durch den Werth $t = 1$ befriedigt. Es giebt nach den Resultaten des vorigen Paragraphen also ein $(z_{11}, z_{21}, \cdots z_{m1}, 1)$, welches alle $f_\alpha = 0$ macht; d. h. die $f_\alpha = 0$ in $z_1, z_2, \cdots z_m$ haben eine gemeinsame Wurzel. $\varrho_0 = 0$ ist charakteristisch für die Existenz gemeinsamer Wurzeln der $(m+1)$ Gleichungen $f_1 = 0, \cdots f_{m+1} = 0$. Da dasselbe für die irreductible Function stattfindet, welche wir als Resultante definirt haben, so kann ϱ_0 nur eine Potenz der Resultanten sein. Ist dies aber im allgemeinen Falle eine höhere als die erste Potenz, so muss es auch in jedem besonderen Falle so sein. Es zeigt aber das Beispiel

$$z_1^{n_1} - a t^{n_1} = 0, \quad z_1^{n_2} - z_1 t^{n_2 - 1} = 0, \cdots z_m^{n_m} - z_{m-1} t^{n_m - 1} = 0;$$
$$z_m^{n_{m+1}} - b t^{n_{m+1}} = 0,$$

dass ϱ_0 in

$$\varrho_0 t^l = (a^{n_{m+1}} - b^k) t^l$$

keine höhere Potenz ist. Damit ist gezeigt: Die Resultante des Systems

$$f_\alpha(z_1, z_2, \cdots z_m) = 0 \quad (\alpha = 1, 2, \cdots m+1)$$

ist in der Form darstellbar

$$\varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_{m+1} f_{m+1} = \varrho_0.$$

§ 418. Wenn zwischen Functionen $f_1, f_2, \cdots f_m$ eine Beziehung

$$\psi_1 f_1 + \psi_2 f_2 + \cdots + \psi_m f_m = H(z_m)$$

besteht, bei der H irreductibel ist, so wird die durch (11^a) definirte Eliminante R ein Vielfaches von H. Nun verschwindet aber R nur für alle die $z_{m\alpha}$, welche aus den Coordinaten der Wurzeln von (1) entnommen werden; für alle diese verschwindet auch H. Folglich muss $R(z_m)$ eine Potenz von $H(z_m)$ sein.

Dies wenden wir auf die $\varphi_1, \varphi_2, \cdots \varphi_m$ in (11^a) selbst an, wobei unter den f_α allgemeine Functionen verstanden werden sollen, R also irreductibel ist. Es folgt, dass die Eliminante von $\varphi_1, \varphi_2, \cdots \varphi_m$ eine

Potenz von $R(z_m)$ wird. Aus den Gradzahlen findet man auch sofort den Exponenten: Die Eliminante von $\varphi_1, \varphi_2, \cdots \varphi_m$ nach z_m ist gleich

$$R(z_m)^q \qquad q = (n_2 n_3 \cdots n_m - 1)(n_1 n_3 \cdots n_m - 1) \cdots (n_1 n_2 \cdots n_{m-1} - 1).$$

Allgemein zeigt sich, dass für ein System

$$f_1^{\delta_1} \varphi_1^{\varepsilon_1}, \quad f_2^{\delta_2} \varphi_2^{\varepsilon_2}, \quad \cdots \quad f_m^{\delta_m} \varphi_m^{\varepsilon_m},$$

in dem jedes δ und ε einen der Werte 0 und 1 haben darf, doch so, dass nicht δ_α und ε_α gleichzeitig Null werden, die Eliminante eine Potenz von $R(z_m)$ ist.

§ 419. Bézout hat seine Methode eingehend durchgearbeitet, ohne jedoch über die durch Constantenabzählung erlangten Möglichkeitsbeweise hinauszugehen. Insbesondere ist er auch auf unvollständige Gleichungen eingegangen, d. h. auf solche, bei denen einzelne Terme fehlen, und hat für sie obere Grenzen der Wurzelzahl gegeben. Ohne darauf näher einzugehen, wollen wir zur Charakterisirung seiner Sätze noch das folgende Theorem anführen*): Sind die Gleichungen (1) so beschaffen, dass in jedem f_α die Variablen

$$z_1, z_2, \cdots \text{ bis zu den Graden } \nu_1^{(\alpha)}, \nu_2^{(\alpha)}, \cdots \qquad (\alpha = 1, 2, \cdots m)$$

aufsteigen, wobei die Summe je zweier dieser Gradzahlen grösser als n_α ist, dann kann man Factoren φ_α so bestimmen, dass (11) besteht, und der Grad von G in z_m den Werth

$$\begin{aligned} n_1 n_2 \cdots n_m &- (n_1 - \nu_1')(n_2 - \nu_1'') \cdots (n_m - \nu_1^{(m)}) \\ &- (n_1 - \nu_2')(n_2 - \nu_2'') \cdots (n_m - \nu_2^{(m)}) \\ &- (n_1 - \nu_3')(n_2 - \nu_3'') \cdots (n_m - \nu_3^{(m)}) \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

nicht übertrifft.

§ 420. Zum Schlusse dieser Vorlesung wollen wir noch eine Erweiterung des Satzes aus § 88, Bd. I geben. Dort gelang es uns, jede Potenz z^k als lineare Function von $1, z, z^2, \cdots z^{n-1}$ auszudrücken, wenn z einer Gleichung n^{ten} Grades genügte, oder mit anderen Worten, wir konnten eine Congruenz

$$z^k \equiv A_0 + A_1 z + A_2 z^2 + \cdots + A_{n-1} z^{n-1} \quad (\text{mod. } f(z))$$

ansetzen, in welcher die A Constanten bedeuten, und $f(z)$ eine Function n^{ten} Grades repräsentirt.

Sind jetzt unsere m Gleichungen (1) gegeben, so wollen wir sie so geordnet denken, dass $n_1 \leqq n_2 \leqq \cdots \leqq n_m$ ist. Man kann dann jeden Ausdruck $z_1^{k_1} z_2^{k_2} \cdots z_m^{k_m}$ als Aggregat ähnlicher Glieder ausdrücken,

*) Équations algébriques; § 62; p. 45.

bei denen jedes $k_\alpha \leq n_\alpha - 1$ ist, oder mit andern Worten, wenn wir wieder die Congruenzbezeichnung benutzen, wir können jede Function

$$F(z_1, z_2, \cdots z_m) \equiv \sum A_h z_1^{h_1} z_2^{h_2} \cdots z_m^{h_m} \quad (\text{modd. } f_1, f_2, \cdots f_m)$$
$$(h_\alpha \leqq n_\alpha - 1;\ \alpha = 1, 2, \cdots m)$$

darstellen. Der Versuch, die Herleitung dieses Resultates auf dem für eine Variable benutzten elementaren Wege zu liefern, stösst schon im einfachsten Falle von zwei Variablen auf merkliche Schwierigkeiten, wie das auch Serret, von welchem diese Ueberlegungen stammen*), bemerkt hat. Auch neuerliche Versuche nach dieser Richtung sind missglückt**).

Wir wollen Factoren $\varphi_1, \varphi_2, \cdots \varphi_m$ so zu bestimmen suchen, dass in

$$F + \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m \tag{22}$$

alle Glieder wegfallen, welche durch $z_1^{n_1}$ oder $z_2^{n_2}, \cdots$ oder $z_m^{n_m}$ theilbar sind. Die Dimension von F nennen wir n_0; F sei eine vollständige Function mit unbestimmten Coefficienten. Für die $\varphi_1, \varphi_2, \cdots \varphi_m$ wählen wir Functionen der Dimensionen $n_0 - n_1, n_0 - n_2, \cdots n_0 - n_m$. Dann haben wir in ihnen zur Verfügung

$$\sum_\alpha N(n_0 - n_\alpha, m) \qquad (\alpha = 1, 2, \cdots m)$$

Constanten. Die Zahl der Potenzproducte in (22) beträgt $N(n_0, m)$; von diesen sollen getilgt werden (vgl. § 331; (7*))

$$N(n_0, m) - \Delta^{(m)}_{n_1, \cdots n_m} N(n_0, m),$$

und so viele Bedingungsgleichungen sind also zu erfüllen. Um das identische Verschwinden des zurückbleibenden Ausdrucks brauchen wir hier natürlich nicht besorgt zu sein. Nach § 333, (11) wird

$$\sum_\alpha N(n_0 - n_\alpha, m) > N(n_0, m) - \Delta^{(m)}_{n_1, \cdots n_m} N(n_0, m) \quad (\alpha = 1, 2, \cdots m),$$

d. h. die Anzahl der zu erfüllenden Gleichungen ist kleiner als die der vorhandenen verfügbaren Constanten. Die Lösungsmöglichkeit ist also im allgemeinen Falle dargethan, wenn sie an einem besonderen Systeme der f_α bei allgemeinen Constanten der Function F gezeigt werden kann.

Genau eine solche Reduction haben wir nun bereits in § 411 durchgeführt. Es braucht nur die dortige Dimension $(n_1 \cdot n_2 \cdots n_m)$ durch n_0 ersetzt zu werden; dann können wir durchaus so verfahren, wie

---

*) l. c. p. 151.

**) Laurent: Traité d'analyse I. Paris (1885), p. 307. In seinem Traité d'Algèbre. Complément IV; Paris (1894) übergeht Laurent diese Frage.

dort geschehen ist. Damit ist bewiesen: Bedeutet F eine Function n_0^{ter} Dimension von $z_1, z_2, \cdots z_m$, dann kann man Functionen φ_α der Dimension $(n_0 - n_\alpha)$ so bestimmen, dass das Aggregat

(20) $$F + \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_m f_m = \Phi$$

durch keins der Monome

$$z_1^{n_1}, \ z_2^{n_2}, \cdots z_m^{n_m}$$

theilbar ist. Solche Functionen Φ nennen wir: nach dem Modulsysteme f_α reducirte Functionen.

Vierzigste Vorlesung.

Eigenschaften der Eliminanten und der Resultanten.

§ 421. Wir nehmen wieder $(m+1)$ allgemeine Gleichungen $f_\alpha = 0$ mit m Variablen und den unbestimmten Coefficienten a_α an; die Dimension von f_α sei n_α; das Product $n_1 \cdot n_2 \cdots n_{m+1}$ bezeichnen wir mit l. Wir bilden die Resultante

(1) $$R = R(f_1, f_2, \cdots f_{m+1}).$$

Einige der Eigenschaften von R haben wir bereits kennen gelernt. Die wichtigsten derselben sind:

I. R ist in den a_α homogen vom Grade $\frac{l}{n_\alpha}$ für $\alpha = 1, 2, \cdots m+1$.

II. R ist in allen Coefficienten isobarisch vom Gewichte l.

III. Es ist

(2) $$R(f_1' \cdot f_1'', f_2, \cdots f_{m+1}) = R(f_1', f_2, \cdots f_{m+1}) \cdot R(f_1'', f_2, \cdots f_{m+1}).$$

Wir wollen zunächst einige Differentialgleichungen ableiten, denen R genügt. Der Einfachheit halber nehmen wir vier Gleichungen mit drei Unbekannten und setzen die Glieder derselben in $f_1, f_2, \cdots$ bez.

$$a'_{\varkappa\lambda\mu} z_1^\varkappa z_2^\lambda z_3^\mu, \quad a''_{\varkappa\lambda\mu} z_1^\varkappa z_2^\lambda z_3^\mu, \cdots.$$

Tragen wir nun in die f für z_1, z_2, z_3 bez. $z_1 + t, z_2 + t, z_3 + t$ ein, so wird die Eigenschaft des Systems $f_\alpha = 0$, gemeinsame Wurzeln zu besitzen oder nicht zu besitzen, dadurch nicht geändert. Für jedes Coefficientensystem, durch welches das ursprüngliche R Null wird, verschwindet also auch das neue; und da jenes R irreductibel, und dieses von gleicher Dimension mit jenem ist, so haben beide Systeme

$$f_\alpha(z_1, \cdots) = 0 \quad \text{und} \quad f_\alpha(z_1 + t, \cdots) = 0$$

das gleiche R als Resultante.

Durch die angegebene Substitution geht $a_{\varkappa\lambda\mu} z_1^\varkappa z_2^\lambda z_3^\mu$ in

$$a_{\varkappa\lambda\mu}(z_1+t)^\varkappa(z_2+t)^\lambda(z_3+t)^\mu$$
$$= a_{\varkappa\lambda\mu}[z_1^\varkappa z_2^\lambda z_3^\mu + (\varkappa z_1^{\varkappa-1} z_2^\lambda z_3^\mu + \lambda z_1^\varkappa z_2^{\lambda-1} z_3^\mu + \cdots)t + \cdots]$$

über, und daraus folgt, dass $a_{\varkappa\lambda\mu}$ im neuen Systeme durch

$$a_{\varkappa\lambda\mu} + [(\varkappa+1)a_{\varkappa+1,\lambda,\mu} + (\lambda+1)a_{\varkappa,\lambda+1,\mu} + (\mu+1)a_{\varkappa,\lambda,\mu+1}]t + \cdots$$

zu ersetzen ist. Vergleicht man nun im alten und im neuen R die Coefficienten der ersten Potenzen von t, dann folgt für R die Differentialgleichung

$$(3)\quad \sum \frac{\partial R}{\partial a_{\varkappa\lambda\mu}}[(\varkappa+1)a_{\varkappa+1,\lambda,\mu} + (\lambda+1)a_{\varkappa,\lambda+1,\mu} + (\mu+1)a_{\varkappa,\lambda,\mu+1}] = 0,$$

wobei die Summe auf alle Elemente a aller vier Gleichungen zu erstrecken ist.

§ 422. Es möge ferner $n_1 \geq n_2$ sein. Ersetzen wir dann $f_1(z_1, z_2, z_3)$ durch $f_1(z_1, z_2, z_3) + tf_2(z_1, z_2, z_3)$, so bleibt die Resultante des neuen Systems der des alten gleich; der Coefficient $a'_{\varkappa\lambda\mu}$ von $z_1^\varkappa z_2^\lambda z_3^\mu$ wird dabei, falls $(\varkappa+\lambda+\mu) > n_2$ ist, ungeändert bleiben, dagegen, falls $(\varkappa+\lambda+\mu) \leq n_2$ ist, durch $a'_{\varkappa\lambda\mu} + ta''_{\varkappa\lambda\mu}$ ersetzt werden. Daraus folgt durch Entwickelung der Resultante nach Potenzen von t: Für R besteht die Differentialgleichung

$$(4)\qquad \sum \frac{\partial R}{\partial a'_{\varkappa\lambda\mu}} a''_{\varkappa\lambda\mu} = 0 \qquad (\varkappa+\lambda+\mu \leq n_2).$$

Die hier benutzte Methode kann leicht verallgemeinert werden, indem man nämlich, ohne R zu ändern, f_1 durch $f_1 + f_2 \cdot \varphi(z_1, z_2, z_3)$ ersetzt, wobei φ eine ganze Function ist, die bis zur Dimension $(n_1 - n_2)$ aufsteigt (vgl. § 398). Aus jeder derartigen Annahme kann man eine Differentialgleichung herleiten, welche von der Natur der Gleichung (4) ist.

§ 423. In f_1 mögen die beiden Glieder

$$a'_{\alpha\beta\gamma} z_1^\alpha z_2^\beta z_3^\gamma \quad \text{und} \quad a'_{\delta\varepsilon\zeta} z_1^\delta z_2^\varepsilon z_3^\zeta$$

vorkommen. Die Resultante R von $f_1 = 0, \cdots f_4 = 0$ sei gleich Null. Wir ändern $a'_{\alpha\beta\gamma}$ und $a'_{\delta\varepsilon\zeta}$ derart ab, dass die Bedingung $R = 0$ gewahrt bleibt, während die beiden betrachteten Coefficienten in

$$a'_{\alpha\beta\gamma} + \sigma \quad \text{und} \quad a'_{\delta\varepsilon\zeta} + \tau$$

übergehen. Wegen $R = 0$ muss also sein

$$(5)\qquad \frac{\partial R}{\partial a'_{\alpha\beta\gamma}}\sigma + \frac{\partial R}{\partial a'_{\delta\varepsilon\zeta}}\tau = 0.$$

Andrerseits ist durch $f_2 = 0, \cdots f_4 = 0$ die gemeinsame Wurzel z_{11}, z_{21}, z_{31} bestimmt, oder vielmehr sie ist nur unter einer

endlichen Zahl von Werthsystemen auszuwählen. Daher wird nicht allein

$$f_1(z_{11}, z_{21}, z_{31}) = \cdots + a'_{\alpha\beta\gamma} z_{11}^{\alpha} z_{21}^{\beta} z_{31}^{\gamma} + a'_{\delta\varepsilon\zeta} z_{11}^{\delta} z_{21}^{\varepsilon} z_{31}^{\zeta} + \cdots = 0,$$

sondern auch

$$\cdots + (a'_{\alpha\beta\gamma} + \sigma) z_{11}^{\alpha} z_{21}^{\beta} z_{31}^{\gamma} + (a'_{\delta\varepsilon\zeta} + \tau) z_{11}^{\delta} z_{21}^{\varepsilon} z_{31}^{\zeta} + \cdots = 0$$

und daraus ergiebt sich durch Subtraction

$$(6) \qquad z_{11}^{\alpha} z_{21}^{\beta} z_{31}^{\gamma} \cdot \sigma + z_{11}^{\delta} z_{21}^{\varepsilon} z_{31}^{\zeta} \cdot \tau = 0.$$

Aus (5) und (6) schliessen wir

$$(7) \qquad \frac{\partial R}{\partial a'_{\alpha\beta\gamma}} : \frac{\partial R}{\partial a'_{\delta\varepsilon\zeta}} = (z_{11}^{\alpha} z_{21}^{\beta} z_{31}^{\gamma}) : (z_{11}^{\delta} z_{21}^{\varepsilon} z_{31}^{\zeta});$$

und derartige Gleichungen gelten für alle Coefficienten a. Aus ihnen folgt, wenn z. B. $\delta = \alpha - 1$; $\varepsilon = \beta$; $\zeta = \gamma$ genommen wird, der Werth der Coordinate z_{11}, u. s. w. Mit Hülfe von (7) lassen sich also die Coordinaten der gemeinsamen Wurzel berechnen. Dabei ist natürlich zu beachten, dass diese Methode beim Vorhandensein mehrerer Wurzeln für $f_1 = 0, \cdots f_{m+1} = 0$ versagt; denn da R eine rationale Function der a ist, kann die linke Seite von (7) nicht mehrdeutig werden. Man darf hieraus also den Schluss ziehen, dass bei mehreren Wurzeln neben $R = 0$ für jeden Coefficienten a auch

$$\frac{\partial R}{\partial a} = 0$$

ist.

§ 424. Für die folgenden Paragraphen wollen wir der Einfachheit halber die $(m+1)$ Gleichungen $f_1 = 0, \cdots f_{m+1} = 0$ unter Wahrung der Dimensionen durch Einführung einer neuen Variabeln z_{m+1} homogen machen. In den f führen wir jetzt die lineare umkehrbare Substitution mit constanten Coefficienten

$$(8) \qquad \begin{aligned} z_1 &= c_{11} v_1 + c_{12} v_2 + c_{13} v_3 + \cdots \\ z_2 &= c_{21} v_1 + c_{22} v_2 + c_{23} v_3 + \cdots \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

durch, bei welcher dann die Determinante $D = |c_{\varkappa\lambda}|$ von Null verschieden ist. Hierdurch verwandele sich f_α in $g_\alpha(v_1, v_2, \cdots)$; die Coefficienten der g_α sind ganze Functionen der $c_{\varkappa\lambda}$ und der a_α. Da die $g_\alpha = 0$ nur dann gemeinsame Wurzeln besitzen, wenn die $f_\alpha = 0$ solche haben und umgekehrt, und da $R(f_1, f_2 \cdots)$ irreductibel ist, so folgt, dass die Resultante von $g_1 = 0, \cdots g_{m+1} = 0$, die wir mit $R(g_1, g_2, \cdots)$ bezeichnen, abgesehen von einem allein von den c abhängigen Factor, eine Potenz von $R(f_1, f_2, \cdots)$ ist. Aus dem Umstande, dass die Coefficienten der g_α linear in den a_α sind, folgt zunächst,

dass die Dimensionen beider Resultanten in den a übereinstimmen, so dass der Exponent jener Potenz nur 1 sein kann. Um den allein von den c abhängigen Factor zu bestimmen, nehmen wir für die f_α besondere Functionen an; wir ersetzen jedes f_α durch ein Product aus n_α allgemeinen homogenen linearen Factoren von $z_1, z_2, \cdots z_{m+1}$. Die Resultante $R(f_1, \cdots)$ wandelt sich in das Product aus den $l = n_1 \cdot n_2 \cdots n_{m+1}$ Determinanten um, die bei Zusammenfassung je eines Factors von f_1, von $f_2, \cdots$ von f_{m+1} entstehen; das folgt aus der Bedeutung von R. Durch (8) reproducirt sich jede dieser Determinanten multiplicirt mit D. Demnach haben wir: Durch die Substitution (8) erhalten wir

$$(9) \qquad R(g_1, g_2, \cdots g_{m+1}) = D^l \cdot R(f_1, f_2, \cdots f_{m+1}).$$

Dieser Satz entspricht dem in § 147, Bd. I abgeleiteten.

Auch für das am Schlusse von § 146, Bd. I gegebene Theorem können wir ein Analogon ausfindig machen. Wir setzen $f_1, f_2, \cdots f_{m+1}$ als von gleicher Dimension n voraus und nehmen

$$g_\alpha = q_{\alpha 1} f_1 + q_{\alpha 2} f_2 + \cdots + q_{\alpha, m+1} f_{m+1} \qquad (\alpha = 1, 2, \cdots m+1)$$

mit constanten q, die eine umkehrbare Substitution bilden. Dann erkennen wir genau wie soeben, dass die beiden Resultanten $R(f_1, f_2, \cdots f_{m+1})$ und $R(g_1, g_2, \cdots g_{m+1})$ sich nur durch einen von den Coefficienten der f unabhängigen Factor unterscheiden können. Genau wie beim vorigen Satze bestimmen wir diesen Factor hier durch ein besonderes System der f. Wir nehmen zu diesem Zwecke

$$f_\alpha = a_{\alpha 1} z_1^n + a_{\alpha 2} z_2^n + \cdots + a_{\alpha, m+1} z_{m+1}^n \qquad (\alpha = 1, 2, \cdots m+1).$$

Dann ersieht man, dass die Determinante der a der einzige Factor von $R(f_1, \cdots)$ sein kann, und die Kenntniss der Dimension zeigt uns

$$R(f_1, f_2, \cdots f_{m+1}) = |a_{\varkappa\lambda}|^{n^m}.$$

Eine einfache Vergleichung mit den Resultaten der Substitution der g liefert, falls $|q_{\varkappa\lambda}| = \varDelta$ gesetzt wird,

$$(9^a) \qquad R(g_1, g_2, \cdots g_{m+1}) = \varDelta^{n^m} R(f_1, f_2, \cdots f_{m+1}).$$

§ 425. Aus der Structur der Eliminante kann ein geometrisch besonders wichtiger Satz ohne Schwierigkeit abgelesen werden, den Liouville zuerst aufgefunden und bewiesen hat*).

Wir waren auf folgendem Wege zur Eliminante $R(z_{m+1})$ von $(m+1)$ Gleichungen mit ebensovielen Unbekannten $z_1, z_2, \cdots z_{m+1}$ gelangt. Zunächst hatten wir $(m+1)$ Gleichungen mit m Unbekannten $z_1, z_2, \cdots z_m$ angenommen und hatten ihre Resultante $R(f_1, \cdots f_{m+1})$ gebildet. Diese war eine isobarische Function der Coefficienten aller

*) J. d. Math. p. e. a. (1) 6 (1841), p. 359.

$f_1, \cdots f_{m+1}$ vom Gewichte $l = n_1 \cdot n_2 \cdots n_{m+1}$, falls den a_α solche Gewichte gegeben werden, dass bei der Annahme der Gewichte 1 für die Unbekannten jedes f_α isobarisch vom Gewichte n_α wird. Eins der Glieder von $R(f_1, f_2, \cdots)$ möge durch

$$(10) \qquad g^{(a)} h^{(b)} k^{(c)} \cdots \qquad (a + b + c + \cdots = l)$$

angedeutet werden. Dabei sollen die $g, h, k, \cdots$ Coefficienten sein, die irgend welchen Functionen f_α angehören, und $a, b, c, \cdots$ sollen die entsprechenden Gewichte andeuten, so dass die Summe $a + b + c + \cdots$ gleich l sein muss.

War so $R(f_1, \cdots f_{m+1})$ gebildet, dann hatten wir in die f_α noch eine neue Unbekannte z_{m+1} dadurch eingeführt, dass wir alle bisherigen Coefficienten a_α durch ganze Functionen von z_{m+1} ersetzten, deren Grad in dieser neuen Unbekannten gleich der Dimension der ersetzten Coefficienten war; also tritt z. B. statt

$$(11) \qquad \begin{array}{lll} g^{(a)} & \text{ein} & g_a + g_{a-1} z_{m+1} + g_{a-2} z_{m+1}^2 + \cdots + g_0 z_{m+1}^a, \\ h^{(b)} & \text{„} & h_b + h_{b-1} z_{m+1} + h_{b-2} z_{m+1}^2 + \cdots + h_0 z_{m+1}^b, \\ k^{(c)} & \text{„} & k_c + k_{c-1} z_{m+1} + k_{c-2} z_{m+1}^2 + \cdots + k_0 z_{m+1}^c, \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{array}$$

wo die unteren Indices der Coefficienten $g, h, k, \cdots$ wieder die Gewichte angeben.

Hierdurch werden die oben angegebenen Resultate über das Gewicht von $R(f_1, \cdots)$ auch für das umgewandelte $R(z_{m+1})$, d. h. für die Eliminante der

$$f_\alpha(z_1, z_2, \cdots z_{m+1}) = 0 \qquad (\alpha = 1, 2, \cdots m + 1)$$

gewahrt bleiben. Man hat also

$$(12) \qquad R(z_{m+1}) = \varrho_0 z_{m+1}^l - \varrho_1 z_{m+1}^{l-1} + \cdots \qquad (l = n_1 \cdot n_2 \cdots n_{m+1}),$$

wobei ϱ_α vom Gewichte α in den Coefficienten isobarisch wird.

Wir wollen, nachdem die Einführung von z_{m+1} vorgenommen ist, die Functionen nach fallenden Dimensionen der Potenzproducte der Unbekannten ordnen:

$$f_\alpha(z_1, \cdots z_{m+1}) = u_{n_\alpha}^{(\alpha)} + u_{n_\alpha - 1}^{(\alpha)} + u_{n_\alpha - 2}^{(\alpha)} + \cdots + u_0^{(\alpha)}$$

wobei $u_\varkappa^{(\alpha)}$ alle Glieder von f_α enthält, die in $z_2, z_2, \cdots z_{m+1}$ von der Dimension $\varkappa$ sind. Die Coefficienten in $u_\varkappa^{(\alpha)}$ müssen daher sämmtlich vom Gewichte $(n_\alpha - \varkappa)$ sein. Es gehören sonach beispielsweise $g_0, h_0, k_0 \cdots$ in (11) zu den Coefficienten von Gliedern der Art $u_{n_\alpha}^{(\alpha)}$; ebenso $g_1, h_1, k_1, \cdots$ zu den Coefficienten von Gliedern der Art $u_{n_\alpha - 1}^{(\alpha)}$; u. s. w. und allgemein $g_\varrho, h_\varrho, k_\varrho, \cdots$ zu den Coefficienten von Gliedern der Art $u_{n_\alpha - \varrho}^{(\alpha)}$.

Trägt man nun (11) in (10) ein, so giebt der Complex aller Ausdrücke (10) die Eliminante (12). ϱ_0 hat das Gewicht 0; folglich können die in ϱ_0 eingehenden Coefficienten nur zu den $g_0, h_0 \cdots$ gehören, d. h. sie entstammen den $u^{(\alpha)}_{n_\alpha}$. Ebenso hat ϱ_1 das Gewicht 1; folglich können die Glieder in ϱ_1 nur von der Form $g_1 h_0 k_0 \cdots$, $g_0 h_1 k_0 \cdots$, $g_0 h_0 k_1 \cdots$, u. s. w. sein, deren Factoren aus den $u^{(\alpha)}_{n_\alpha}$ und den $u^{(\beta)}_{n_\beta - 1}$ entstammen, u. s. w. Das ist der Liouville'sche Satz, dem wir folgenden Ausdruck geben: Der Coefficient ϱ_i von z_{m+1}^{l-i} hängt nur von solchen Coefficienten der f_α ab $(\alpha = 1, 2, \cdots m+1)$, die in Gliedern der Dimensionen n_α, $(n_\alpha - 1), \cdots (n_\alpha - i)$ der Potenzproducte vorkommen. Für ϱ_0 war dies schon bekannt, vgl. § 394.

§ 426. Wie wir früher gezeigt haben, hängen die symmetrischen Functionen der $z_1, z_2, \cdots z_{m+1}$ von den Coefficienten der Eliminantengleichung

$$(13)\quad R(x) = \varrho_0 x^l - \varrho_1(\varkappa_1, \cdots \varkappa_{m+1}) x^{l-1} + \varrho_2(\varkappa_1, \cdots \varkappa_{m+1}) x^{l-2} - \cdots = 0$$
$$(x = \varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_{m+1} z_{m+1})$$

ab. Von den Coefficienten der Gleichung (13) gilt dasselbe, was soeben für die von (12) bewiesen wurde. Nun ergibt sich aus § 379, dass jedes

$$S(z_{11}^{\alpha_1} z_{21}^{\alpha_2} \cdots z_{12}^{\beta_1} z_{22}^{\beta_2} \cdots) \qquad (\Sigma\alpha + \Sigma\beta + \cdots = i)$$

durch ein Aggregat von Producten der Potenzsummen $s_{\varrho\sigma\tau\cdots}$ ausgedrückt werden kann, bei denen $\varrho + \sigma + \tau + \cdots \leqq i$ ist; und aus § 377, (7) folgt, dass diese s aus den zu (13) gehörigen Potenzsummen $S_{\varrho'+\sigma'+\tau'+\cdots}$ der $x_1, x_2, \cdots$ abgeleitet werden können, bei denen $\varrho' + \sigma' + \tau' + \cdots = \varrho + \sigma + \tau \leqq i$ ist. Die S können aus den Coefficienten von (13) dargestellt werden und so erkennen wir: Die symmetrischen Functionen i^{ter} Dimension der Wurzeln von

$$f_\alpha = u^{(\alpha)}_{n_\alpha} + u^{(\alpha)}_{n_\alpha - 1} + \cdots + u^{(\alpha)}_0 = 0 \qquad (\alpha = 1, 2, \cdots m+1)$$

hängen nur von den Coefficienten der Aggregate $u^{(\alpha)}_{n_\alpha}, \cdots u^{(\alpha)}_{n_\alpha - i}$ ab.

Der Liouville'sche Satz ist für die analytische Geometrie von grossem Interesse. Man findet die Anwendungen desselben, so weit sie von Liouville stammen, am angeführten Orte. Weitere, eingehende Studien rühren von Humbert*) und von G. Fouret**) her.

Wir wollen wenigstens ein hierher gehöriges Theorem herleiten, indem wir dabei den Betrachtungen Fouret's folgen:

---

*) J. d. M. p. e. a. (4) 3 (1887), p. 361 und Nouv. Ann. (3) 6 (1887) p. 533.
**) Nouv. Ann. (3) 9 (1890), p. 258.

Der Schwerpunkt der Berührungspunkte aller Tangenten, welche einer gegebenen Richtung parallel an eine algebraische Curve gezogen werden können, ist ein fester, von der Richtung unabhängiger Punkt.

Es sei $f(x, y) = 0$ die Gleichung der Curve, bezogen auf rechtwinklige Coordinaten x und y; sie steige bis zur n^{ten} Dimension auf. Die Berührungspunkte aller Tangenten, welche der Richtung parallel laufen, die mit der positiven Halbaxe der x den Winkel α bildet, befriedigen gleichzeitig die Gleichungen $f = 0$ und

$$\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} \operatorname{tang} \alpha = 0. \tag{14}$$

Nun sei die Eliminante dieser beiden Gleichungen

$$\varrho_0 x^{m(m-1)} - \varrho_1 x^{m(m-1)-1} + \cdots = 0,$$

dann ist die Abscisse des gesuchten Schwerpunktes

$$\xi = \frac{1}{m(m-1)} \frac{\varrho_1}{\varrho_0}.$$

Nach dem Liouville'schen Satze hängen ϱ_0 und ϱ_1 nur von den Gliedern m^{ter} und $(m-1)^{\text{ter}}$ Dimension in f ab, weil diese ja die Glieder $(m-1)^{\text{ter}}$ und $(m-2)^{\text{ter}}$ Dimension in (14) bestimmen. ξ ändert sich daher nicht, wenn man f durch ein f_1 ersetzt, welches in den Gliedern der beiden höchsten Dimensionen mit f übereinstimmt, sonst aber beliebig gebildet ist; es ist also nur nöthig, dass $f = 0$ und $f_1 = 0$ die gleichen Asymptoten haben. Man kann daher insbesondere auch die vorgelegte Curve durch den Complex ihrer Asymptoten selbst ersetzen. Hierbei fallen nun die Berührungspunkte mit den Schnittpunkten der einzelnen Asymptoten untereinander zusammen, und also haben diese sicher das gleiche ξ. Ferner aber sind die Schnittpunkte von α unabhängig; daher ξ ebenfalls, und so ist das aufgestellte Theorem bewiesen. Es ist für die Gültigkeit des Satzes wesentlich, dass die Curve keine parabolischen Zweige hat, da sonst Asymptoten ins Unendliche fallen würden.

§ 427. Zu einer anderen wichtigen Einsicht führen uns unsere Betrachtungen über die Resultante und Eliminante auf folgendem Wege.

Wir gehen von den m Gleichungen mit m Unbekannten

$$f_\alpha(z_1, z_2, \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

aus und führen nach Liouville die Substitution

$$z_m = x - (\varkappa_1 z_1 + \varkappa_2 z_2 + \cdots + \varkappa_{m-1} z_{m-1})$$

durch. Dadurch möge entstehen

$$f_\alpha(z_1, z_2, \cdots z_m) = g_\alpha(z_1, \cdots z_{m-1}; x) \qquad (\alpha = 1, 2, \cdots m). \tag{15}$$

Aus den g bestimmen wir gemäss dem Bézout'schen Verfahren die Eliminante

(16) $$R(x) = g_1 P_1 + g_2 P_2 + \cdots + g_m P_m.$$

Nach Kronecker schreiben wir diese Gleichung bequem als Congruenz

(17) $$R(x) \equiv 0 \quad (\text{modd. } g_1, g_2, \cdots g_m),$$

und von dieser können wir wegen (15) zurückgehen auf

(17ᵃ) $$R(x) \equiv 0 \quad (\text{modd. } f_1, f_1, \cdots f_m).$$

Nun zerlegen wir $R(x)$ in seine linearen Factoren und bedenken dabei, dass jede Wurzel der Gleichung $R = 0$ von der Form

$$\varkappa_1 \zeta_1 + \varkappa_2 \zeta_2 + \cdots + \varkappa_{m-1} \zeta_{m-1} + \zeta_m$$

ist. Es sei R in seine verschiedenen Wurzelfactoren zerlegt

$$R \equiv [\varkappa_1(z_1 - \zeta_{11}) + \varkappa_2(z_2 - \zeta_{21}) + \cdots]^{\mu_1}$$
$$\cdot [\varkappa_1(z_1 - \zeta_{12}) + \varkappa_2(z_2 - \zeta_{22}) + \cdots]^{\mu_2} \cdots \equiv 0.$$

Denkt man sich diesen Ausdruck nach Potenzproducten der $\varkappa$ geordnet, so muss jeder einzelne Coefficient congruent 0 sein, da ja die Glieder f_α des Modulsystems von den $\varkappa$ unabhängig sind.

Der Coefficient von $\varkappa_1^{\mu_1+\mu_2+\cdots}$ liefert dabei

(18ᵃ) $$(z_1 - \zeta_{11})^{\mu_1}(z_1 - \zeta_{12})^{\mu_2} \cdots = (z_1 - \zeta_{11})^{\mu_1} \cdot U_0 \equiv 0 \quad (\text{modd. } f_1, \cdots),$$

und derjenige von $\varkappa^{\mu_1+\mu_2+\cdots-1} \cdot \varkappa_2$ liefert

$$(z_1 - \zeta_{11})^{\mu_1}\left[\mu_1 \frac{z_2 - \zeta_{21}}{z_1 - \zeta_{11}} + \mu_2 \frac{z_2 - \zeta_{22}}{z_1 - \zeta_{12}} + \cdots\right] \cdot U_0 \equiv 0.$$

Multiplicirt man diese Congruenz mit $(z_1 - \zeta_{12})(z_1 - \zeta_{13})\cdots$, so entsteht, da wegen (18ᵃ) alle Glieder, die auf das erste folgen, $\equiv 0$ werden,

(18ᵇ) $$(z_1 - \zeta_{11})^{\mu_1 - 1}(z_2 - \zeta_{21}) \cdot U_1 \equiv 0 \quad (\text{modd. } f_1, \cdots),$$

wobei $U_1 = (z_1 - \zeta_{12})^{\mu_2+1}(z_1 - \zeta_{13})^{\mu_3+1} \cdots$ ist; es reicht also auch schon aus, für U_1 eine hinlänglich hohe Potenz von $(z_1 - \zeta_{12})(z_1 - \zeta_{13})\cdots$ sich zu denken. —

Nun gehen wir zu den Gliedern $\varkappa_1^{\mu_1+\mu_2+\cdots-2}\varkappa_2^2$ in der Entwickelung von R über. Dabei erhalten wir zwei Arten von Gliedern, von deren jeder ein charakteristisches Glied angegeben werden soll:

$$\binom{\mu_1}{2}(z_1 - \zeta_{11})^{\mu_1-2}(z_2 - \zeta_{21})^2 \cdot U;$$
$$\binom{\mu_1}{1}\binom{\mu_2}{1}(z_1 - \zeta_{11})^{\mu_1-1}(z_2 - \zeta_{21})(z_1 - \zeta_{12})^{\mu_2-1}(z_2 - \zeta_{22}) \cdot V_0,$$

wobei V_0 für $(z_1 - \zeta_{13})^{\mu_3}(z_1 - \zeta_{14})^{\mu_4} \cdots$ geschrieben ist. Multiplicirt man alle diese Glieder mit $(z_1 - \zeta_{12})^2(z_1 - \zeta_{13})^2 \cdots$, so werden wegen (18ᵃ) und (18ᵇ) alle einzelnen Producte bis auf das hingeschriebene Erste $= 0$; dieses Erste giebt dann Veranlassung zu der Congruenz

(18^c) $\quad (z_1 - \zeta_{11})^{\mu_1-2}(z_2 - \zeta_{21})^2 \cdot U_2 \equiv 0 \quad (\text{modd.}\, f_1, \cdots),$

wobei U_2 wieder eine passende Potenz von $(z_1 - \zeta_{12})(z_1 - \zeta_{13}) \cdots$ bedeutet. —

In den Coefficienten von $x_1^{\mu_1+\mu_2+\cdots-2} \cdot x_2 \cdot x_3$ treten Glieder von zweierlei Form auf, nämlich erstens

$$\binom{\mu_1}{1}\binom{\mu_2}{1}(z_1 - \zeta_{11})^{\mu_1-1}(z_1 - \zeta_{21}) \cdot (z_1 - \zeta_{12})^{\mu_2-1}(z_3 - \zeta_{32}) \cdot (z_1 - \zeta_{13})^{\mu_3} \cdots,$$

und zweitens

$$\binom{\mu_1}{2}(z_1 - \zeta_{11})^{\mu_1-2}(z_2 - \zeta_{21})(z_3 - \zeta_{31}) \cdot (z_1 - \zeta_{12})^{\mu_2}(z_1 - \zeta_{13})^{\mu_3} \cdots.$$

Multiplicirt man hier mit einer hinlänglich hohen Potenz von $(z_1 - \zeta_{12})(z_1 - \zeta_{13}), \cdots$, so folgt wieder

(18^d) $\quad (z_1 - \zeta_{11})^{\mu_1-2}(z_2 - \zeta_{21})(z_3 - \zeta_{31})\, U \equiv 0 \quad (\text{modd.}\, f_1, \cdots).$

So kann man fortfahren und sieht: Ist U eine hinlänglich hohe Potenz von $(z_1 - \zeta_{12})(z_1 - \zeta_{13}) \cdots$, dann wird

(18) $\quad (z_1 - \zeta_{11})^{\alpha}(z_2 - \zeta_{21})^{\beta}(z_3 - \zeta_{31})^{\gamma} \cdots U \equiv 0 \quad (\text{modd.}\, f_1, f_2, \cdots f_m),$

wenn $(\alpha + \beta + \gamma + \cdots) \geqq \mu_1$ ist; oder auch: man kann setzen

(18*) $\quad (z_1 - \zeta_{11})^{\alpha}(z_2 - f_{21})^{\beta} \cdots U = Q_1 f_1 + Q_2 f_2 + \cdots + Q_m f_m.$

§ 428. Nach Herleitung dieses, als Hülfsatz dienenden Theorems betrachten wir eine Function Φ, welche für alle Wurzeln $(\zeta_{11}, \zeta_{21}, \cdots)$, $(\zeta_{12}, \zeta_{22}, \cdots), \cdots$ des Systems $f_\alpha = 0$ gleich Null wird. Aus § 350, (4) wissen wir, dass dann mit passenden Coefficienten φ

$$\begin{aligned} \Phi &= (z_1 - \zeta_{11})\varphi_{11} + (z_2 - \zeta_{21})\varphi_{12} + (z_3 - \zeta_{31})\varphi_{13} + \cdots \\ &= (z_1 - \zeta_{12})\varphi_{21} + (z_2 - \zeta_{22})\varphi_{22} + (z_3 - \zeta_{32})\varphi_{23} + \cdots \\ &\quad \cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

geschrieben werden kann. Ist nun μ der grösste der Exponenten $\mu_1, \mu_2, \ldots,$ und bildet man $\Phi^\mu \cdot U'$, wobei U' eine hinlänglich hohe Potenz von $(z_1 - \zeta_{12})(z_1 - \zeta_{13}) \cdots$ ist, so enthält jedes der Glieder des entwickelten Ausdrucks

$$[(z_1 - \zeta_{11})\varphi_{11} + (z_2 - \zeta_{21})\varphi_{12} + (z_3 - \zeta_{31})\varphi_{13} + \cdots]^\mu \cdot U'$$

Factoren von der Form (18), und daher ist

(19) $\quad \Phi^\mu \cdot U' \equiv 0 \quad (\text{modd.}\, f_1, f_2, \cdots f_{m+1});$

ebenso folgt, wenn man $\zeta_{11}, \zeta_{21}, \cdots$ mit $\zeta_{12}, \zeta_{22}, \cdots$ vertauscht,

(19^a) $\quad \Phi^\mu \cdot U'' \equiv 0 \quad (\text{modd.}\, f_1, f_2, \cdots f_m),$

wobei U'' eine Potenz von $(z_1 - \zeta_{11})(z_1 - \zeta_{13}) \cdots$ bedeutet; ferner

(19^b) $\quad \Phi^\mu \cdot U''' \equiv 0 \quad (\text{modd.}\, f_1, f_2, \cdots f_m),$

wobei U''' eine Potenz von $(z_1 - \zeta_{11})(z_1 - \zeta_{12})(z_1 - \zeta_{14}) \cdots$ sein wird; u. s. f.

Die mit U', U'', U''', $\cdots$ bezeichneten Functionen der z_1, z_2, $\cdots$ haben in ihrer Gesammtheit keinen gemeinsamen Factor. Folglich kann man Functionen $v', v'', v''', \cdots$ von $z_1, z_2, \cdots$ derart bestimmen, dass

$$v'U' + v''U'' + v'''U''' + \cdots = 1$$

wird (§ 346; XII). Multiplicirt man (19), (19ᵃ), (19ᵇ), $\cdots$ der Reihe nach mit v', v'', v''', $\cdots$ und addirt die Producte, so entsteht

$$\Phi^\mu \equiv 0 \qquad (\text{modd. } f_1, f_2, \cdots f_m) \tag{20}$$

oder ausführlich geschrieben

$$\Phi^\mu = f_1 Q_1 + f_2 Q_2 + \cdots + f_m Q_m. \tag{20ᵃ}$$

Die v', v'', $\cdots$ werden noch ζ_{11}, ζ_{12}, $\cdots$ enthalten, und dasselbe gilt auch von den Factoren Q_1, Q_2, $\cdots$. Nun kann man aber in (20ᵃ) die ζ_{11}, ζ_{12}, $\cdots$ beliebig untereinander vertauschen. Thut man dies, addirt sämmtliche hierdurch entstehenden Gleichungen und bedenkt, dass dann die Factoren der f_α in den Wurzeln symmetrisch werden, so folgt, dass man sie rational in den Coefficienten der f_α darstellen kann. Demnach können wir den Satz aussprechen: **Wenn eine Function Φ für alle, in endlicher Anzahl vorhandenen Wurzeln des Systems**

$$f_\alpha(z_1, z_2 \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

verschwindet, dann kann die Gleichung

$$\Phi^\mu = f_1 Q_1 + f_2 Q_2 + \cdots + f_m Q_m \tag{20ᵃ}$$

aufgestellt werden, in welcher die Q_i ganze Functionen der z mit rationalen Coefficienten bedeuten und μ die höchste vorkommende Multiplicität einer Wurzel ist*). Es ist ersichtlich, dass dieser Satz von hoher Bedeutung für die Geometrie der Curven und Flächen ist; $\Phi = 0$ stellt dabei eine Curve oder eine Fläche dar, welche durch alle Durchschnittspunkte der Curven oder Flächen $f_\alpha = 0$ hindurchgeht.

§ 429. Bei den Untersuchungen der letzten beiden Paragraphen stimmte die Zahl der Gleichungen $f_\alpha = 0$ mit derjenigen der Unbekannten z überein. Wir können uns von dieser Voraussetzung frei machen. In der That, wenn die Anzahl m' der Variabeln geringer ist als die Anzahl m der Gleichungen, während doch noch eine endliche

---

*) Herr Noether hat dieses Theorem in dem Aufsatze: „Ueber einen Satz aus der Theorie der algebraischen Functionen" für $m = 2$ in etwas anderer, für unsere Zwecke weniger geeigneten Form abgeleitet. (Math. Ann. 6 (1852) p. 351.) Vgl. auch E. Bertini: Math. Ann. 34 (1889), p. 447; und 35 (1889), p. 456; ferner Noether: Math. Ann. 34 (1839), p. 450 und E. Netto: Acta math. 7 (1885), p. 101.

Anzahl von Wurzeln besteht, dann können wir mit willkürlichen Parametern $u_{\varkappa\lambda}$ neue Functionen

$$g_\alpha = u_{\alpha 1} f_1 + u_{\alpha 2} f_2 + \cdots + u_{\alpha m} f_m \qquad (\alpha = 1, 2, \cdots m')$$

ableiten, welche wegen der Unbestimmtheit der $u_{\varkappa\lambda}$ nur für die Wurzeln der $f_\alpha = 0$ verschwinden und für alle diese Wurzeln. Daraus folgt

$$\Phi^\mu = g_1 Q_1 + g_2 Q_2 + \cdots + g_{m'} Q_{m'}.$$

Die Q sind hier rational in den Coefficienten der f und in den $u_{\varkappa\lambda}$. Für unbestimmte u verschwinden die etwa auftretenden Nenner nicht identisch, und folglich giebt es besondere Zahlenwerthe, für welche dies auch nicht der Fall ist (§ 337). Trägt man diese ein und geht auf die f zurück, dann ist der Satz des vorigen Paragraphen von der Voraussetzung befreit, dass die Zahl der Variablen mit derjenigen der Gleichungen übereinstimmen müsse.

§ 430. Wir können jetzt auch die Voraussetzung fallen lassen, dass die Gleichungen $f_\alpha = 0$ nur eine endliche Anzahl von Wurzeln besitzen. Es seien m Functionen f_α mit $(p+1)$ Variablen gegeben. Das Theorem über die Darstellbarkeit sei bereits für m Functionen und p Variable bewiesen; wir wollen daraus herleiten, dass es auch für m Functionen mit $(p+1)$ Variablen gilt. Da wir bei der Beschränkung auf hinreichend wenige Variable zu einer endlichen Anzahl von Wurzeln kommen, weil sonst das System $f_\alpha = 0$ identisch erfüllt wäre, so ist damit der allgemeine Satz bewiesen. Die Variablen seien $z_1, z_2, \cdots z_p, z_{p+1}$. Wir betrachten z_{p+1} als Parameter, dem wir einen beliebigen endlichen Werth zuertheilt denken. Dann ist der Voraussetzung nach für die p Variablen $z_1, \cdots z_p$

$$\Phi^\mu = P_1 f_1 + P_2 f_2 + \cdots + P_m f_m;$$

die P sind dabei rational in den Coefficienten der f und in z_{p+1}. Der Hauptnenner der P sei $\varrho(z_{p+1})$; dann können wir schreiben

$$\varrho(z_{p+1}) \cdot \Phi^\mu = Q_1 f_1 + Q_2 f_2 + \cdots + Q_m f_m. \tag{21}$$

Genau in der gleichen Art können wir herleiten

$$\begin{aligned} \sigma(z_1) \cdot \Phi^\mu &= R_1 f_1 + R_2 f_2 + \cdots + R_m f_m, \\ \tau(z_2) \cdot \Phi^\mu &= S_1 f_1 + S_2 f_2 + \cdots + S_m f_m, \\ &\cdots\cdots\cdots \end{aligned} \tag{21*}$$

wobei offenbar das μ in allen Gleichungen als dasselbe angenommen werden kann, da es ja in jeder solchen Gleichung beliebig vergrössert werden darf.

Das System

$$f_1 = 0, \cdots f_m = 0; \quad \sigma(z_1) = 0, \quad \tau(z_2) = 0, \cdots \varrho(z_{p+1}) = 0$$

hat wegen seiner letzten $(p+1)$ Gleichungen offenbar eine endliche Anzahl von Wurzeln, die wegen der ersten m Gleichungen sämmtlich Φ zum Verschwinden bringen. Folglich ist

$$\Phi^{\nu} = M_1 f_1 + M_2 f_2 + \cdots + M_m f_m + N_1 \sigma(z_1) + N_2 \tau(z_2) + \cdots + N_{p+1}\, \varrho(z_{p+1})$$

und also, wenn man mit Φ^{μ} multiplicirt und die Gleichungen (21) und (21*) verwendet,

$$\Phi^{\nu+\mu} \equiv 0 \quad (\text{modd. } f_1, f_2, \cdots f_m).$$

Damit ist der allgemeine Satz bewiesen*).

§ 431. Es mögen jetzt m vollständige allgemeine Functionen $f_1, f_2, \cdots f_m$ von den $(m+p)$ Variabeln $z_1, z_2, \cdots z_m;\ v_1, v_2, \cdots v_p$ gegeben sein. Ferner sei Φ eine Function derselben Variabeln, und φ eine Function allein von $v_1, v_2, \cdots v_p$. Wir nehmen an, dass das Product $\Phi(z_1, \cdots z_m;\ v_1, \cdots v_p) \cdot \varphi(v_1, \cdots v_p)$ für alle Wurzeln von $f_1 = 0, \cdots f_m = 0$ verschwinde.

Eine solche Wurzel sei $(z_{11}, \cdots z_{m1},\ v_{11}, \cdots v_{p1})$. Dann können wir (§ 350)

$$(22) \qquad \Phi = C + (z_1 - z_{11})\psi_1 + \cdots$$
$$+ (z_m - z_{m1})\psi_m + (v_1 - v_{11})\chi_1 + \cdots + (v_p - v_{p1})\chi_p$$

setzen, wobei C von Null verschieden ist, wenn Φ nicht selbst schon für diese Wurzel $(z_{11}, \cdots v_{p1})$ verschwindet. Jetzt wählen wir $v_{22}, \cdots v_{p2}$ den Werthen $v_{21}, \cdots v_{p1}$ beliebig benachbart und auch v_{12} dem v_{11} beliebig nahe, aber so, dass nicht $\varphi(v_{12}, v_{22}, \cdots v_{p2}) = 0$ ist. Dies geht bei passender Anordnung der v stets, wenn φ nicht identisch verschwindet. Wir können bei dieser Wahl direct festsetzen, dass

$$|v_{12} - v_{11}|, \quad |v_{22} - v_{21}|, \cdots |v_{p2} - v_{p1}| < \delta_1$$

sein soll, wo δ_1 beliebig klein sein mag.

Jetzt bestimmen wir weiter $z_{12}, \cdots z_{m2}$ so, dass für diese Werthe

$$f_\alpha(z_1, \cdots z_m,\ v_{12},\ v_{22}, \cdots v_{p2}) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

wird, was angeht, da die Anzahl der Gleichungen derjenigen der Unbekannten gleich kommt, und da trotz der Einführung von $v_{12}, \cdots v_{p2}$ die f_α als Functionen der z aufgefasst, nach wie vor allgemein und vollständig sind. Nach § 353 werden auch $|z_{12} - z_{11}|, \cdots |z_{m2} - z_{m1}|$ bei hinreichend kleinem δ_1 beliebig klein. Wir können alle absoluten Beträge der Differenzen zweier Coordinaten $< \delta_0$ machen, wo δ_0 mit δ_1 gleichzeitig unendlich klein wird. Für den Bereich der durch

*) Diese und noch weitergehende Verallgemeinerungen des Problems der Darstellung stammen von Herrn Hilbert: „Ueber die vollen Invariantensysteme". Math. Ann. 42 (1892), p. 320. Der hier gegebene Beweis ist dieser Arbeit entnommen.

$$|z_1 - z_{11}|, \quad |z_2 - z_{21}|, \cdots |z_m - z_{m1}|, \cdots |v_p - v_{p1}| < \delta_0$$

bestimmten $z_1, \cdots z_m, v_1, \cdots v_p$ seien $\Psi_1, \cdots \Psi_m, X_1, \cdots X_p$ die Maxima der absoluten Beträge von $\psi_1 \cdots \psi_m, \chi_1, \cdots \chi_p$ aus (22) und Ω sei der grösste aller dieser Beträge.

Da $z_{12}, \cdots z_{m2}, v_{12} \cdots v_{p2}$ eine Wurzel des Systems $f_\alpha = 0$ ist, so wird für sie $\Phi . \varphi = 0$, und weil $\varphi \neq 0$ ist, so wird $\Phi = 0$, d. h. nach (22)

$$C + (z_{12} - z_{11})\psi_1 + \cdots + (z_m - z_{m1})\psi_m (v_{12} - v_{11})\chi_1 + \cdots + (v_{p2} - v_{p1})\chi_p = 0.$$

Der absolute Betrag der linken Seite ist grösser als

$$|C| - \Sigma|(z_{\alpha 2} - z_{\alpha 1})\psi_\alpha| - \Sigma|(v_{\beta 2} - v_{\beta 1})\chi_\beta| \geqq |C| - (m + p)\delta_0 \Omega.$$

Durch Verringerung von δ_1 kann man dies wesentlich positiv machen, falls $|C|$ nicht verschwindet. Dann wäre aber $\Phi \neq 0$, und folglich ist $C = 0$. Das heisst: Verschwindet das Product

$$\Phi(z_1, \cdots z_m, v_1, \cdots v_p) \cdot \varphi(v_1, \cdots v_p)$$

für alle Wurzeln des Systems

$$f_\alpha(z_1, \cdots z_m, v_1, \cdots v_p) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

von m Gleichungen mit $(m + p)$ Unbekannten, dann verschwindet auch schon Φ allein für alle diese Wurzeln; deshalb ist auch hier

$$\Phi = f_1 Q_1 + f_2 Q_2 + \cdots + f_m Q_m.$$

Einundvierzigste Vorlesung.

Kronecker's Eliminationsmethode. — Reductibilität und Irreductibilität.

§ 432. Sind $z_{11}, z_{12}, \cdots z_{1n}$ irgend welche Grössen, deren symmetrische Functionen dem Rationalitätsbereiche angehören, so ist es leicht, alle Gleichungen aufzustellen, deren Coefficienten gleichfalls dem Rationalitätsbereiche zugehören, und unter deren Wurzeln $z_{11}, z_{12}, \cdots z_{1n}$ sich befinden. Die einfachste dieser Gleichungen ist diejenige, welche auch keine weiteren Wurzeln besitzt, nämlich

$$f(z_1) \equiv (z_1 - z_{11})(z_1 - z_{12}) \cdots (z_1 - z_{1n}) = 0,$$

und die übrigen werden durch $f(z_1) \cdot \varphi(z_1) = 0$ geliefert, wobei $\varphi(z_1)$ eine beliebige ganze Function des Rationalitätsbereiches bedeutet.

Die nächstliegende, dieser Aufgabe entsprechende, auf ein System von Gleichungen bezügliche Frage würde die folgende sein. Es sind

k Werthsysteme $(z_{1\alpha}, z_{2\alpha}, \cdots z_{m\alpha})$ für $\alpha = 1, 2, \cdots k$ der m Variablen $z_1, z_2, \cdots z_m$ gegeben. Es sollen alle Gleichungssysteme mit rational bekannten Coefficienten gefunden werden, welche jene Werthsysteme und keine andern zu Wurzeln haben. Diese Aufgabe lässt unendlich viele Lösungen zu. Man könnte sie z. B. so behandeln, dass zuerst ein

$$(1) \qquad f(z_1) \equiv (z_1 - z_{11})(z_1 - z_{12}) \cdots (z_1 - z_{1k}) = 0$$

bestimmt wird; dann könnte man mit Hülfe der **Lagrange**'schen Interpolationsformel jedem $z_1 = z_{1\alpha}$ ein $z_2 = z_{2\alpha}$ vermittels

$$(2) \qquad f_2(z_1, z_2) \equiv z_2 - \sum_\alpha z_{2\alpha} \frac{f(z_1)}{(z_1 - z_{1\alpha})f'(z_{1\alpha})} = 0$$

zuordnen; ähnlich jedem $z_{1\alpha}$ ein $z_{3\alpha}$, u. s. f. In dieser Art lassen sich also m Gleichungen herstellen, die das Problem lösen. Jede lineare Combination derselben wird im Allgemeinen das Gleiche thun. Man darf dabei aber nicht vergessen, dass das aufgestellte System noch fremde, im Unendlichen gelegene Wurzeln besitzt. Sind z. B. vorgeschrieben

$$(z_1, z_2) = (-1, 0), \ (0, 1), \ (1, 0),$$

dann findet man nach der angegebenen Vorschrift

$$f_1 \equiv z_1^3 - z_1 = 0; \quad f_2 \equiv z_1^2 + z_2 - 1 = 0,$$

so dass ausser jenen drei endlichen Wurzeln noch drei unendlich grosse bestehen. Dieser Uebelstand wird sich im Allgemeinen überhaupt nicht heben lassen; das erkennt man schon aus unserem Beispiele. Der **Bézout**'sche Satz zeigt, dass die drei Wurzeln nur dann das volle Wurzelsystem zweier Gleichungen ausmachen können, wenn $n_1 = 3$, $n_2 = 1$ ist; jene drei Wurzeln können aber nicht einer linearen Gleichung Genüge leisten.

Hat man auf verschiedene Arten die Darstellung einer Reihe von Werthsystemen als Wurzeln geleistet, z. B. durch

$$f_1 = 0, \ f_2 = 0, \cdots \quad \text{und durch} \quad g_1 = 0, \ g_2 = 0, \cdots,$$

dann wird jedes f für alle Wurzeln des zweiten Systems gleich Null werden und umgekehrt. Nach dem Schlussparagraphen der letzten Vorlesung giebt es also Darstellungen

$$f_\alpha^{\mu_\alpha} = P'_\alpha g_1 + P''_\alpha g_2 + \cdots \qquad (\alpha = 1, 2, \cdots);$$

$$g_\alpha^{\nu_\alpha} = Q'_\alpha f_1 + Q''_\alpha f_2 + \cdots \qquad (\alpha = 1, 2, \cdots).$$

§ 433. Im Falle, dass mehrere Gleichungen mit mehreren Unbekannten vorliegen, braucht sich aber „das Gemeinsame" des Systems nicht auf einzelne Werthsysteme in endlicher Anzahl zu beschränken (vgl. § 404). Es können z. B. bei drei Variablen — geometrisch

gesprochen — nicht nur gemeinsame Punkte der Gebilde vorhanden sein, sondern auch gemeinsame Curven, ja sogar gemeinsame Flächenstücke. Man erkennt, dass in jedem der letztern Fälle die Darstellung (1), (2) versagen würde, da ja (1) für unendlich viele Wurzeln erfüllt wäre, also $f(z_1)$ identisch verschwinden müsste.

Zugleich ist es klar, dass das ganze Problem hier anders gefasst werden muss. Die allgemeine Fragestellung ist die: Es sind beliebig viele Gleichungen

$$(3) \quad f_1(z_1, \cdots z_m) = 0, \quad f_2(z_1, \cdots z_m) = 0, \cdots f_q(z_1, \cdots z_m) = 0$$

zwischen m Variablen $z_1, \cdots z_m$ gegeben. Welche Einschränkungen werden durch die Gleichungen (3) auf die m-fache Mannigfaltigkeit der z ausgeübt? Insbesondere: Wieviele Gleichungen sind höchstens nothwendig, um die durch (3) definirten Gebilde rein darzustellen?

In dieser umfassenden und weitblickenden Form hat L. Kronecker*) das Eliminationsproblem behandelt. Wir geben im Folgenden die Hauptgesichtspunkte wieder. Gleich hier sei von vornherein darauf aufmerksam gemacht, dass die Frage nach der Multiplicität von Lösungen ganz zurücktritt.

§ 434. Zunächst führen wir wieder nach Liouville

$$(4) \quad z_m = x - (u_1 z_1 + \cdots + u_{m-1} z_{m-1}); \quad x = u_1 z_1 + \cdots + u_m z_m \quad (u_m = 1)$$

in (3) ein und erhalten dadurch statt $f_1, f_2, \cdots$

$$(5) \quad g_1(x; z_1, \cdots z_{m-1}) = 0, \quad g_2(x; z_1, \cdots z_{m-1}) = 0, \cdots.$$

Die f nehmen wir als präparirt an, um Besonderheiten auszuschalten (§ 355). Es wird dadurch z. B. vermieden, dass nur einzelne Coordinaten einer Wurzel unendlich gross werden. Ebenso können nicht zu einem System $z_1, z_2, \cdots z_{m-1}$ unendlich viele Werthe z_m gehören.

Den grössten gemeinsamen Theiler von $g_1, g_2, \cdots$ befreien wir von etwa vorhandenen mehrfachen Factoren, benennen die zurückbleibende Function $R_1(x; z_1, \cdots z_{m-1})$ und bezeichnen mit G_α die in R_1 nicht enthaltenen Factoren von g_α. Dann entsprechen, abgesehen von der Multiplicität der Wurzeln, allen Lösungen von (5) alle von

$$(6) \quad R_1(x; z_1, z_2, \cdots z_{m-1}) = 0;$$

$$(6^a) \quad G_1(x; z_1, \cdots z_{m-1}) = 0, \quad G_2(x; z_1, \cdots z_{m-1}) = 0, \cdots;$$

und umgekehrt entspricht jeder Lösung von (6) oder von (6^a) eine solche von (5). Es kann also aus jeder Lösung von (3) eine solche

---

*) Grundzüge einer arithm. Theorie u. s. w. J. f. M. 92 (1882), p. 1, § 10. Vgl. auch die ausführlichen Erläuterungen von J. Molk: Acta math. 6 (1885), p. 1.

von (6) oder (6ª) hergeleitet werden; und umgekehrt lässt sich zu jeder von (6) oder von (6ª) ein z_m so bestimmen, dass man eine Lösung von (3) erhält. Daraus folgt, dass bei der Zerlegung von R_1 in lineare Factoren nach x

$$R_1 = (x-\xi)(x-\xi')\cdots = (u_1 z_1 + \cdots + u_m z_m - \xi)(u_1 z_1 + \cdots + u_m z_m - \xi')\cdots$$

jedes ξ, ξ', $\cdots$ linear und homogen in $u_1, \cdots u_m$ ist. Denn zu $x = \xi$; $z_1, \cdots z_{m-1}$ giebt es ein $z_m = \xi - (u_1 z_1 + \cdots + u_{m-1} z_{m-1})$, welches mit $z_1, \cdots z_{m-1}$ zusammen eine Wurzel von (5) giebt. Diese Wurzeln sind von $u_1, \cdots u_{m-1}$ unabhängig; demnach ist

$$\xi = u_1 z_1 + \cdots + u_{m-1} z_{m-1} + \zeta_m.$$

Man hat deswegen

$$R_1 = (x - u_1 z_1 - \cdots - u_{m-1} z_{m-1} - \zeta_m)(x - u_1 z_1 - \cdots - u_{m-1} z_{m-1} - \zeta'_m)\cdots$$
$$= (z_m - \zeta_m)(z_m - \zeta'_m)\cdots,$$

und die $\zeta_m, \zeta'_m, \cdots$ sind Wurzeln einer Gleichung, deren Coefficienten rational von $z_1, z_2, \cdots z_{m-1}$ abhängen. Die durch (6) erlangten Wurzeln von (3) bilden also eine Mannigfaltigkeit $(m-1)^{\text{ter}}$ Dimension. In ihnen lassen sich $z_1, z_2, \cdots z_{m-1}$ beliebig wählen, z_m ist dadurch bestimmt.

Alle nicht hierdurch gelieferten Wurzeln von (3) befriedigen (6ª). Wir bilden mit unbestimmten Parametern v und w zwei Functionen

6ᵇ) $\quad v_1 G_1 + v_2 G_2 + \cdots + v_q G_q, \qquad w_1 G_1 + w_2 G_2 + \cdots + w_q G_q.$

Wenn ein System $(\xi_1, \zeta_1, \cdots \zeta_{m-1})$ beide für jede Wahl der v, w zu Null macht, dann ist (6ª) befriedigt, und umgekehrt macht jede Wurzel von (6ª) die beiden Functionen (6ᵇ) zu Null. Wir eliminiren aus beiden die Grösse z_{m-1} und ordnen die Eliminante nach Potenzproducten der v, w. Die Coefficienten mögen

(7) $\qquad h_1(x; z_1, \cdots z_{m-2}) = 0, \quad h_2(x; z_1, \cdots z_{m-2}) = 0, \cdots$

sein, auf deren Anzahl es nicht weiter ankommt. Jede Lösung von (6ª) liefert hiernach eine solche von (7); umgekehrt kann zu jeder Wurzel $(\xi, \zeta_1, \cdots \zeta_{m-2})$ von (7) ein ζ_{m-1} so gefunden werden, dass $(\xi, \zeta_1, \cdots \zeta_{m-1})$ jene beiden linearen Gleichungen (6ᵇ) in v, w und also auch (6ª) befriedigt. Dieses ζ_{m-1} scheint, da es von (6ᵇ) abhängt, eine Function der v, w zu sein; deshalb wollen wir $\zeta_{m-1}(v, w)$ schreiben. Dann wären

$$\xi, \zeta_1, \cdots \zeta_{m-2}, \zeta_{m-1}(v, w)$$

die Coordinaten einer Wurzel von (6ª). Von diesen Wurzeln kennen wir bereits die Form; sie haben die Coordinaten

$$\xi = u_1 \zeta_1 + \cdots + u_m \zeta_m, \ \zeta_1, \zeta_2, \cdots \zeta_{m-2}, \zeta_{m-1}.$$

Daraus folgt, dass ζ_{m-2} von v, w unabhängig ist, da es ja schon in ξ als Coefficient von u_{m-1} auftritt. Die durch (6) nicht gegebenen Wurzeln von (3) werden demnach von (7) geliefert.

Den grössten gemeinsamen Theiler von $h_1, h_2, \cdots$ befreien wir von etwa vorhandenen mehrfachen Factoren, benennen die zurückbleibende Function $R_2(x; z_1, \cdots z_{m-2})$ und führen ähnlich wie oben die H_α ein. Dann entsprechen, abgesehen von der Multiplicität der Wurzeln, allen Lösungen von (7) alle von

$$(8) \qquad R_2(x; z_1, z_2, \cdots z_{m-2}) = 0;$$

$$(8^a) \quad H_1(x; z_1, \cdots z_{m-2}) = 0, \quad H_2(x; z_1, \cdots z_{m-2}) = 0, \cdots;$$

und umgekehrt entspricht jeder Lösung von (8) oder von (8ᵃ) eine solche von (7). Daraus folgt, dass alle Wurzeln von (8) oder von (8ᵃ) Coordinaten von der Form

$$\xi = u_1\zeta_1 + u_2\zeta_2 + \cdots + u_m\zeta_m, \ \zeta_1, \zeta_2, \cdots \zeta_{m-2}$$

haben. Nun schliesst man wie oben, dass

$$R_2 = [u_{m-1}(z_{m-1} - \zeta_{m-1}) + (z_m - \zeta_m)][u_{m-1}(z_{m-1} - \zeta'_{m-1}) + (z_m - \zeta'_m)] \cdots$$

sein wird. Die durch (8) erlangten Wurzeln von (9) bilden also eine Mannigfaltigkeit $(m-2)^{\text{ter}}$ Dimension. In ihnen sind $z_1, z_2, \cdots z_{m-2}$ beliebig; z_{m-1} und z_m werden als Wurzeln von $R_2 = 0$ durch sie bestimmt.

Alle nicht durch (6) und (8) gegebenen Wurzeln von (3) werden durch (8ᵃ) geliefert. An dieses System knüpfen wir dieselben Betrachtungen wie oben an (6ᵃ). Man kann demgemäss durch Fortsetzung des Verfahrens folgenden Satz beweisen: Sämmtliche verschiedenen Wurzeln von

$$(3) \quad f_1(z_1, \cdots z_m) = 0, \quad f_2(z_1, \cdots z_m) = 0, \cdots f_q(z_1, \cdots z_m) = 0$$

werden durch eine der Gleichungen

$$R_\alpha(x; z_1, z_2, \cdots z_{m-\alpha}) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

geliefert. Hierbei bedeutet x den Ausdruck $u_1 z_1 + u_2 z_2 + \cdots + u_{m-1} z_{m-1} + z_m$. Die durch $R_\alpha = 0$ gegebenen Wurzeln bilden eine Mannigfaltigkeit $(m-\alpha)^{\text{ter}}$ Dimension; es bleiben $z_1, z_2, \cdots z_{m-\alpha}$ beliebig, $z_{m-\alpha+1}, \cdots z_m$ werden durch sie algebraisch bestimmt. Die einzelnen R_α heissen Theileliminanten; das Product

$$R_1 \cdot R_2 \cdots R_m$$

heisst die Gesammteliminante von (3).

Wie man erkennt, sind wir auch hier wieder auf völlig naturgemässem Wege zur Eintheilung der Gebilde ihrer Stufenzahl nach gekommen (§ 405).

§ 435. Nach diesen Ergebnissen sind wir im Stande zu erklären, was man unter der Reductibilität und der Irreductibilität eines Functionen- oder eines Gleichungssystems zu verstehen hat. Ein System von Functionen oder Gleichungen (3) nennen wir irreductibel oder reductibel, je nachdem seine Gesammteliminante es ist.

Daraus folgt sofort: Ist ein Gleichungssystem so beschaffen, dass jede Function, die einen Wurzelpunkt mit ihr gemeinsam hat, für alle seine Wurzeln verschwindet, dann ist das System irreductibel. Denn wäre es reductibel, dann könnte man seine Gesammteliminante zerlegen, $R = S \cdot T$, und die Gleichung $S = 0$ gäbe gegen die Voraussetzung nur einen Theil der Wurzeln.

Dagegen gilt der Satz nicht, dass wenn eine Wurzel eines irreductiblen Systems (3) eine Function $\Phi(z_1, \cdots z_m)$ zum Verschwinden bringt, dann Φ für jede Wurzel von (3) verschwindet, wie man wohl zuerst geneigt wäre, der Analogie gemäss zu schliessen*). Ein einfaches Beispiel zeigt dies; das Gebilde „die Kugel“

$$z_1^2 + z_2^2 + z_3^2 - 1 = 0$$

ist sicher als irreductibles System aufzufassen; dies hat gleichwohl mit

$$z_1 + z_2 + z_3 - 1 = 0$$

Wurzeln gemeinsam, aber nicht sämmtliche. Das wirkliche, den Sätzen mit einer Variablen analoge Theorem würde sich etwas complicirter gestalten, indem eine gemeinsame Wurzel von $\Phi = 0$ und von (3) nur bei zwei Theileliminanten von gleicher Dimension der Mannigfaltigkeit oder von gleicher Stufenzahl entscheidend wird.

§ 436. Die Aufgabe, ein gegebenes System (3) in seine irreductiblen Factoren zu zerlegen, ist hiernach einfach zu lösen. Wir bilden die Gesammteliminante, oder auch das System der Theileliminanten und zerlegen dieses oder jene in alle ihre irreductiblen Factoren

$$S(u_1 z_1 + u_2 z_2 + \cdots + u_m z_m, z_2, z_3, \cdots z_m).$$

Entwickeln wir jetzt nach Potenzproducten der Unbestimmten u, dann liefert das gleich Null gesetzte System der einzelnen Coefficienten ein Gleichungssystem, dessen Inhalt mit dem von $S = 0$ vollkommen übereinstimmt. Diese Darstellung gilt übrigens auch von reductiblen Theilern der Gesammteliminante, ja auch von ihr selbst.

Die Anzahl der durch diese Entwickelung sich ergebenden Coefficienten kann natürlich sehr bedeutend sein. Es lässt sich aber nachweisen, dass $(m+1)$ Functionen stets ausreichen, um eine vollständige

---

*) Herr Molk (l. c.) führt dieses Theorem an (V, § 3) und versucht auch einen Beweis desselben herzuleiten.

Darstellung eines jeden S zu liefern. Das soll im nächsten Paragraphen geschehen.

Aus dem Dargelegten ist ersichtlich, dass die Zerlegung eines Systems in irreductible Systeme nur auf eine Art vor sich gehen kann, wobei freilich nur die dargestellten Mannigfaltigkeiten eindeutig festgelegt werden, nicht aber die darstellenden Functionen der Systeme, weder ihrer Form noch ihrer Anzahl nach.

Ein System ist ein Theiler eines anderen Systems, wenn die Gesammteliminante des ersten ein Theiler derjenigen des zweiten wird.

Ferner wird es klar, was unter theilerfremden Systemen zu verstehen sei, nämlich Gleichungssysteme, deren Gesammteliminanten keinen gemeinsamen Factor haben.

Als grössten gemeinsamen Theiler zweier Systeme haben wir dasjenige System zu definiren, welches durch den gemeinsamen Factor ihrer Gesammteliminanten bestimmt wird.

Aus dieser Definition ergiebt sich sofort weiter, dass zu den beiden Systemen

$$f_1, f_2, \cdots f_q \quad \text{und} \quad \varphi_1, \varphi_2, \cdots \varphi_\varkappa$$

das System, welches aus allen $(q + \varkappa)$ Elementen f und φ besteht, der grösste gemeinsame Theiler ist.

§ 437. Wir wollen jetzt den angekündigten Satz beweisen, dass wenn irgend ein System (3) vorgelegt ist, sein Gesammtinhalt durch höchstens $(m + 1)$ Gleichungen vollständig ausgedrückt werden kann.

Wir betrachten irgend einen Theiler der Gesammteliminante von (3), der nicht nothwendig irreductibel zu sein braucht. Durch sein Verschwinden werde eine $(m - \alpha)$-fache Mannigfaltigkeit definirt, die aber auch mit Mannigfaltigkeiten niederer Dimensionen gemischt auftreten kann. Wir bezeichnen diesen Theiler der Gesammteliminante mit

$$(9) \qquad S_\alpha(u_1 z_1 + \cdots + u_m z_m,\ z_1,\ z_2, \cdots z_{m-\alpha}) = 0.$$

Setzen wir hierin der Reihe nach alle u mit Ausnahme zuerst von $u_{m-\alpha+1}$, dann von $u_{m-\alpha+2}, \cdots$ endlich von u_m gleich Null, und diese $u_{m-\alpha+1}, \cdots u_m$ gleich 1, so entsteht eine Reihe von Gleichungen

$$(10) \quad \sigma_{m-\alpha+1}(z_{m-\alpha+1};\ z_1, \cdots z_{m-\alpha}) = 0, \cdots\ \sigma_m(z_m;\ z_1, \cdots z_{m-\alpha}) = 0.$$

Es ist klar, dass (9) ein Theiler von (10) ist. Die Gesammteliminante von (10) sei $T(x;\ z_1, \cdots z_m)$; dann wird $S_\alpha(x;\ z_1, \cdots z_{m-\alpha})$ ein Factor von T

$$T(x;\ z_1, \cdots z_m) = S_\alpha(x;\ z_1, \cdots z_{m-\alpha})\, U(x;\ z_1, \cdots z_m).$$

Da, wie gewöhnlich, mehrfache Wurzeln ausgeschaltet sind, so haben S_α und U keinen Theiler bei allgemeinen $u_1, u_2, \cdots u_m$ gemeinsam. Wir schreiben jetzt

$$S_\alpha(x;\, z_1, \cdots z_{m-\alpha}) = S'_\alpha(z_1, z_2, \cdots z_m;\, u_1, u_2 . \cdots u_m).$$

Durch jeden gleich Null gesetzten Factor von U wird eine Mannigfaltigkeit definirt, welche z. B.

$$z_{\beta+1} = \chi_1(z_1, \cdots z_\beta), \quad z_{\beta+2} = \chi_2(z_1, \cdots z_\beta), \cdots$$

bestimmt. Es sind die χ mehrwerthige algebraische Functionen, d. h. Wurzeln algebraischer Gleichungen. Tragen wir alle diese Werthe in S'_α ein und multipliciren wir die Resultate, dann haben wir eine Function, die in $z_{\beta+1}, z_{\beta+2}, \cdots$ symmetrisch, also durch $z_1, \cdots z_\beta$ und die Coefficienten jener Gleichungen darstellbar ist. In diesem Producte kommen somit nur die Variablen $z_1, \cdots z_\beta;\, u_1, \cdots u_m$ vor; und bei unbestimmten u ist das Product von Null verschieden, weil $S_\alpha = 0$ mit $U = 0$ keinen gemeinsamen Theiler hat. Da das Product bei unbestimmten $u_1, \cdots u_m$ nicht verschwindet, so kann man auch besondere Werthe ausfindig machen, für welche dies nicht geschieht. Ordnet man nämlich nach Potenzproducten der $z_1, \cdots z_\beta$, so brauchen die u nur so gewählt zu werden, dass nicht alle Coefficienten dieser Potenzproducte verschwinden.

Führt man diese Operationen bei allen Factoren von U durch, dann gelangt man zu besonderen Constanten $u_1 = p_1, \cdots u_m = p_m$, für welche keins der Producte der S'_α, also auch kein S_α selbst infolge von $U = 0$ verschwindet.

Daher wird auch für diese Constanten die Gleichung

$$(11) \qquad S_\alpha(p_1 z_1 + p_2 z_2 + \cdots + p_m z_m;\, z_1, \cdots z_{m-\alpha}) = 0$$

mit $U = 0$ keine Wurzel mehr gemeinsam haben, und (10) und (11) liefern zusammen $(\alpha + 1)$ Gleichungen, welche den Inhalt von (9) rein und vollständig wiedergeben.

Eine reine oder gemischte Theileliminante, durch welche keine höheren als $(m - \alpha)$-fache Mannigfaltigkeiten definirt werden, kann vollständig und rein durch $(\alpha + 1)$ Gleichungen dargestellt werden. Insbesondere: Jedes beliebige Gleichungssystem (3) zwischen m Variablen kann vollständig und rein durch höchstens $(m + 1)$ Gleichungen dargestellt werden.

Die Bedeutung dieses Satzes für die analytische Geometrie liegt auf der Hand. Er zeigt z. B., dass Raumcurven rein erst durch vier Gleichungen zwischen den drei Coordinaten dargestellt werden können, oder dass eine beliebige Anzahl von Punkten in der Ebene erst als Durchschnittssystem dreier Curven rein geliefert werden wird.

Es ist klar, dass $(\alpha + 1)$ Gleichungen bei der Darstellung zwar stets ausreichen, aber nicht immer nothwendig sind, um eine Mannig-

faltigkeit $(m-\alpha)^{\text{ter}}$ Ordnung rein anzugeben. Man kann ja eine solche direct durch α Gleichungen zwischen den m Variablen z definiren.

Zweiundvierzigste Vorlesung.

Abhängigkeit und Unabhängigkeit von Functionen und von Gleichungen. — Die Functionaldeterminante.

§ 438. Sind zwei Functionen einer Variablen z gegeben

$$a_0 z^m + a_1 z^{m-1} + \cdots + a_m, \quad b_0 z^n + b_1 z^{n-1} + \cdots + b_n,$$

und bezeichnet man ihre Werthe für ein willkürliches z mit φ und ψ, so sind die Gleichungen

$$a_0 z^m + a_1 z^{m-1} + \cdots - \varphi = 0, \quad b_0 z^n + b_1 z^{n-1} + \cdots - \psi = 0$$

gleichzeitig für jenes z erfüllt, und infolge dessen ist

$$\begin{vmatrix} a_m - \varphi & a_{m-1} & a_{m-2} & \cdots \\ 0 & a_m - \varphi & a_{m-1} & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ b_n - \psi & b_{n-1} & b_{n-2} & \cdots \\ 0 & b_n - \psi & b_{n-1} & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix} = C_0 \cdot \varphi^n + C_1 \cdot \varphi^{n-1}\psi + \cdots = 0,$$

d. h. es besteht eine Gleichung zwischen φ und ψ, deren Coefficienten Constanten sind, und die nicht für alle beliebigen Werthe von φ, ψ erfüllt sein kann. Diese Thatsache, dass die Werte der beiden Functionen nicht unabhängig von einander gewählt werden können, sprechen wir so aus, dass wir sagen, die Functionen seien nicht von einander unabhängig.

Sind q Functionen von m Variablen

$$(1) \qquad f_1(z_1, \cdots z_m), \quad f_2(z_1, \cdots z_m), \cdots f_q(z_1, \cdots z_m)$$

gegeben, dann heissen sie unabhängig von einander, wenn keine Gleichung

$$(2) \qquad F(f_1, f_2, \cdots f_q) = 0$$

besteht, deren Coefficienten von den Variablen unabhängig sind, und die nicht identisch erfüllt ist, d. h. nicht, wenn man f_1, f_2, $\cdots f_q$ als beliebige variable Grössen ansieht. Es sind also Gleichungen, wie etwa

$$f_1^2 + (f_2 - f_1)(f_2 + f_1) - f_2^2 = 0$$

nicht geeignet, eine Abhängigkeit zu begründen.

Besteht zwischen den $f_1, \cdots f_q$ eine solche Gleichung (2), dann können nicht alle Werthe für $f_1, \cdots f_q$ beliebig gewählt werden, da sie ja eben (2) befriedigen müssen. Kann man umgekehrt das System $z_1, z_2, \cdots z_m$ so wählen, dass $f_1, \cdots f_q$ jedes willkürlich vorgeschriebene Werthsystem annehmen kann, dann besteht natürlich keine Gleichung (2) zwischen den Functionalwerthen, und die Functionen sind von einander unabhängig. Von diesem an sich klaren Satze haben wir schon früher Gebrauch gemacht.

§ 439. Es möge zunächst die Anzahl der Gleichungen diejenige der Variablen um 1 übertreffen, also $q = m + 1$ sein. Giebt man den Variablen ein beliebiges Werthsystem, dann mögen die Werthe der Functionen durch die Symbole $\varphi_1, \varphi_2, \cdots \varphi_q$ bezeichnet werden. Es sind folglich die Gleichungen

$$(3) \qquad f_\alpha(z_1, z_2, \cdots z_m) - \varphi_\alpha = 0 \quad (\alpha = 1, 2, \cdots m+1)$$

mit einander verträglich, und ihre Resultante R ist daher $= 0$. Diese ist eine ganze Function der Coefficienten aller f und zugleich der Werthe $\varphi_1, \varphi_2, \cdots \varphi_q$. Wir beweisen, dass R nicht identisch verschwinden kann, d. h. nicht dann, wenn man $\varphi_1, \cdots \varphi_q$ als unabhängige Variable auffasst.

Nach der Poisson'schen Bildungsweise für Resultanten ist

$$R = \prod_\alpha [f_{m+1}(z_{1\alpha}, \cdots z_{m\alpha}) - \varphi_{m+1}],$$

wobei die $(z_{1\alpha}, \cdots z_{m\alpha})$ alle endlichen Wurzeln der Gleichungen

$$f_\varrho(z_{1\alpha}, \cdots z_{m\alpha}) - \varphi_\varrho = 0 \quad (\varrho = 1, 2, \cdots m)$$

zu durchlaufen haben. Aus dieser Poisson'schen Productform ist ersichtlich, dass in R die Grösse φ_{m+1} nicht verschwinden kann. Das Gleiche gilt für alle übrigen φ_ϱ. Unter Andeutung dieser Grössen schreiben wir für die Resultantengleichung

$$R(\varphi_1, \varphi_2, \cdots \varphi_{m+1}) = 0,$$

oder, da die φ ja nur eingeführt waren, um ohne Irrthümer und Zweideutigkeiten die $f_1, \cdots f_{m+1}$ darzustellen, so erhält man jetzt eine Gleichung von der Gestalt der Relation (2), nämlich

$$(4) \qquad R(f_1, f_2, \cdots f_{m+1}) = 0.$$

Ist die Anzahl der Functionen um eins grösser als die Anzahl der Variablen, dann besteht zwischen ihnen eine Gleichung (2), welche aus der Resultante des Gleichungssystems (3) hergeleitet werden kann. Daraus folgt: Uebertrifft die Anzahl der Functionen diejenige der Variablen, dann bestehen mindestens so viele Relationen (2), als die Differenz der beiden

Anzahlen beträgt. Wir werden in der nächsten Vorlesung mit der Aufstellung derartiger Relationen zu thun haben und uns mit dem Problem beschäftigen, ein System unabhängiger Relationen aufzustellen.

Die Function auf der linken Seite von (4) hat nur dann ein von den $f_1, f_2, \cdots f_{m+1}$ freies Glied, wenn das System

$$f_1 = 0, \; f_2 = 0, \; \cdots \; f_{m+1} = 0$$

eine Wurzel besitzt; bei allgemeinen Functionen findet das also nicht statt.

§ 440. Ist $q > m$, dann giebt es stets Relationen (2); es ist aber nicht ausgeschlossen, dass derartige Gleichungen auch für $q \leqq m$ auftreten, dass es also auch dann eine Gleichung $F(f_1, \cdots f_q) = 0$ giebt.

Wir wollen annehmen, dieser Umstand trete ein; dabei können wir voraussetzen, dass wir nur diejenigen Functionen f_α in Betracht ziehen, welche wirklich in F eingehen, indem wir die übrigen einfach von unserer Betrachtung ausschliessen. Wir können ferner die Voraussetzung machen, dass nicht schon unter weniger als q Functionen $f_1, f_2, \cdots f_q$ eine Beziehung dieser Art stattfindet, da wir sonst unsere Schlüsse sofort an diese geringere Zahl knüpfen könnten. Dann kann man das System mit willkürlichen $\varphi_1, \varphi_2, \cdots \varphi_{q-1}$

$$(5) \qquad f_\alpha(z_1, z_2, \cdots z_m) - \varphi_\alpha = 0 \quad (\alpha = 1, 2, \cdots q-1)$$

befriedigen. Denn wenn man anderenfalls $q-2$ Variable eliminirt, so fallen in der Eliminante alle Variablen fort, weil sie für keine Wahl derselben verschwinden dürfte, und sie selbst liefert gleich Null gesetzt eine Relation zwischen den f_α.

Bei (5) ist es möglich, dass $(q-1)$ der m Variablen z bestimmt oder auch durch die übrigen ausgedrückt werden; $m - q + 1$ bleiben unbestimmt. Jene $(q-1)$ eliminiren wir aus (5) und

$$(5^a) \qquad f_q(z_1, z_2, \cdots z_m) - \varphi_q = 0,$$

wobei φ_q einen Werth bezeichnet, der mit der Einschränkung der z durch (5) verträglich ist. Nun sind die Gleichungen (5) und (5^a) gleichzeitig erfüllbar; ihre Resultante nach $(q-1)$ Variablen $z_{m-q+2}, \cdots z_m$ ist also Null. So erhalten wir $R = 0$, wobei in R ausser den Coefficienten der f_α noch die Werte φ_α und die unbestimmt gebliebenen Variablen $z_1, \cdots z_{m-q+1}$ eingehen können. Wir entwickeln R nach Potenzproducten der $\varphi_1, \cdots \varphi_q$; dabei entstehe

$$(6) \qquad R = \sum_{(\beta)} A_\beta \varphi_1^{\beta_1} \varphi_2^{\beta_2} \cdots \varphi_q^{\beta_q} = 0.$$

Jetzt sollte der Voraussetzung nach eine von den Variablen freie Gleichung

$$(6^a) \qquad F(f_1, f_2, \cdots f_{q-1}, f_q) = 0$$

bestehen. Setzen wir in ihr $f_1 = \varphi_1, \cdots f_{q-1} = \varphi_{q-1}$, so bestimmt sich daraus f_q als Wurzel einer algebraischen Gleichung; d. h. zu jedem System $\varphi_1, \cdots \varphi_{q-1}$ giebt es nur eine endliche Anzahl von Werthen φ_q, und diese sind frei von $z_1, \cdots z_{m-q+1}$ bestimmt, was aus (5^a) noch nicht hervorging. Dies wirft ein neues Licht auf (6). Kommt in den A_β in (6) eine der Variablen $z_1, \cdots z_{m-q+1}$ wirklich vor, dann kann man nach der bei (5) gemachten Bemerkung für unendlich viele Werthe derselben festgegebene Werthe von $\varphi_1, \cdots \varphi_{q-1}$ erhalten und dann durch (6^a) die möglichen Werthe von φ_q bestimmen. Für die festen $\varphi_1, \cdots \varphi_{q-1}$ und für ein unter einer endlichen Anzahl von Werthen vorkommendes φ_q müsste (6) bei unendlich vielen Werthen der wirklich in den A_β vorkommenden Variablen befriedigt werden. Es giebt daher auch unendlich viele Werthe dieser Variablen, für die (6) bei festem $\varphi_1, \varphi_2, \cdots \varphi_{q-1}$ und festem φ_q gilt. Folglich müssten alle Coefficienten A_β identisch verschwinden, und da dies ausgeschlossen ist, so kann keine der Variablen $z_1, \cdots z_{m-q+1}$ in die Coefficienten A_β eingehen. Die übrigen Variablen aber waren eliminirt; folglich ist R in seinen Coefficienten ganz von den Variablen frei, und $R = 0$ eine Relation wie sie gesucht wurde. So haben wir ein Mittel erlangt, ein Functionensystem darauf hin zu prüfen, ob eine Abhängigkeit zwischen seinen Elementen besteht, und wenn dies der Fall ist, solche Relationen (2) auch wirklich aufzustellen. Um zu untersuchen, ob die q Functionen $f_1, \cdots f_q$ von m ($\geqq q$) Variablen $z_1, z_2, \cdots z_m$ ein unabhängiges oder ein abhängiges System bilden, bestimme man auf alle Arten die Eliminante in Beziehung auf die Elimination von $(q-1)$ Variablen zwischen den Gleichungen

$$f_\alpha(z_1, \cdots z_m) - \varphi_\alpha = 0 \qquad (\alpha = 1, 2, \cdots q),$$

wobei die φ_α lediglich Bezeichnungen für die f_α sind. Ist eine dieser Eliminanten auch von den übrigen Variablen unabhängig, dann und nur dann bilden die f ein abhängiges System, und diese Eliminante liefert direct die zwischen den f bestehende Relation.

§ 441. Jacobi hat in seiner Abhandlung „de determinantibus functionalibus" (Werke III, p. 393) die Frage nach der Abhängigkeit von Functionen oder von Gleichungen untereinander von anderen Gesichtspunkten her behandelt. Er setzt dabei nicht voraus, dass es sich gerade um ganze Functionen oder um algebraische Gleichungen handelt; als Haupttheorem stellt er das folgende auf, durch welches die Abhängigkeit oder Unabhängigkeit von m Functionen ebensovieler Variablen erkannt wird.

Sind m Functionen $f_\alpha(z_1, z_2, \cdots z_m)$ für $\alpha = 1, 2, \cdots m$ vorgelegt, so heisst die Determinante

$$J = \left| \frac{\partial f_\varkappa}{\partial z_\lambda} \right| = \frac{\partial(f_1, f_2, \cdots f_m)}{\partial(z_1, z_2, \cdots z_m)} \qquad (\varkappa, \lambda = 1, 2, \cdots m)$$

die Functionaldeterminante des Systems. Englische Mathematiker bezeichnen sie als „Jacobian“. Wir sind dieser Determinante schon im § 399 begegnet. Ihr Verschwinden für eine Wurzel $(z_{11}, \cdots z_{m1})$ der $f_\alpha = 0$ war charakteristisch dafür, dass die Wurzel eine mehrfache Wurzel des Systems ist. Jacobi beweist von ihr: Das identische Verschwinden der Functionaldeterminante ist charakteristisch für den Umstand, dass die Functionen nicht von einander unabhängig sind. Den analytisch gehaltenen Beweis Jacobi's wollen wir hier nicht angeben; es sei auf die Originalabhandlung oder auf eine der Darstellungen in Lehrbüchern der Determinantentheorie oder der Analysis verwiesen.

Verbinden wir das Jacobi'sche Resultat mit dem von uns im vorigen Paragraphen hergeleiteten, so folgt eine merkwürdige Beziehung zwischen dem Aufbau der Eliminante und dem der Functionaldeterminante.

Lassen wir zunächst in den Functionen f_α die Coefficienten unbestimmt, eliminiren $z_2, z_3, \cdots z_m$ aus den Gleichungen

$$f_\alpha(z_1, z_2, \cdots z_m) - \varphi_\alpha = 0 \qquad (\alpha = 1, 2, \cdots m),$$

behalten z_1 zurück, ordnen die Eliminante nach z_1 und setzen

$$R(z_1; \varphi_1, \cdots \varphi_m) = \sum_\varkappa \tau_\varkappa(\varphi_1, \cdots \varphi_m) \cdot z_1^\varkappa;$$

schreiben wir dann andrerseits die Functionaldeterminante

$$J = \sum_{\alpha, \beta, \cdots} \varrho_{\alpha\beta\ldots} z_1^\alpha z_2^\beta \cdots,$$

so wird für jede Wahl der Coefficienten in $f_1, f_2, \cdots$, durch welche alle $\varrho_{\alpha\beta\ldots}$ zu Null werden, J identisch verschwinden; folglich bilden die f_α ein abhängiges System, und nach § 440 wird eine der Eliminanten, etwa die obige von z_1 frei; d. h. die $\tau_\varkappa$ $(\varkappa > 1)$ verschwinden. Dass wir hier gerade das obige R nehmen, ist natürlich bei der Allgemeinheit der Coefficienten keine Beschränkung. — Das Umgekehrte findet ebenso statt; denn verschwinden alle diese Coefficienten in R, dann sind die Functionen nicht unabhängig von einander, und infolge dessen sind alle $\varrho_{\alpha\beta\ldots} = 0$. Wir haben also den Satz: Ordnet man

$$R(z_1; \varphi_1, \cdots \varphi_m) = \sum_{\varkappa, \lambda, \cdots} \tau_{\varkappa\lambda\mu\ldots} z_1^\varkappa \varphi_1^\lambda \varphi_2^\mu \cdots,$$

$$J = \sum_{\alpha, \beta, \cdots} \varrho_{\alpha\beta\ldots} z_1^\alpha z_2^\beta \cdots,$$

dann sind Potenzen der $\varrho_{\alpha\beta}\ldots$ homogen und linear durch die $\tau_{\varkappa\lambda\mu}\ldots$ ($\varkappa>0$) darstellbar und umgekehrt Potenzen der $\tau_{\varkappa\lambda}\ldots$ durch die $\varrho_{\alpha\beta}\ldots$.

Wir wollen zwei einfache Beispiele hierzu geben. Es sei zuerst

$$f_1-\varphi_1=z_1^2+2az_1z_2+bz_2^2+2cz_1+2dz_2-\varphi_1,$$
$$f_2-\varphi_2=z_1-\alpha z_2-\varphi_2,$$

dann wird

$$R=(\alpha^2+2\alpha a+b)z_2^2+2((\alpha+a)\varphi_2+c\alpha+d)z_2+(\varphi_2^2-2c\varphi_2-\varphi_1),$$
$$-\frac{1}{2}J=(a+\alpha)z_1+(a\alpha+b)z_2+(\alpha c+d).$$

Hier ist die Richtigkeit des Theorems sofort ersichtlich, da man hat

$$\alpha^2+2\alpha a+b=\alpha(a+\alpha)+(a\alpha+b)$$

und

$$a\alpha+b=(\alpha^2+2\alpha a+b)-\alpha(a+\alpha).$$

Als zweites Beispiel wählen wir

$$f_1-\varphi_1=z_1^2-2az_1z_2+bz_2^2-\varphi_1,$$
$$f_2-\varphi_2=z_1^2-2\alpha z_1z_2+\beta z_2^2-\varphi_2;$$

das giebt für R den Ausdruck

$$[(\beta-b)+(\alpha-a)(\alpha b-\beta a)]z_2^4$$
$$+2[\varphi_1(\beta-b+a\alpha-\alpha^2)+\varphi_2(b-\beta+a\alpha-a^2)]z_2^2+(\varphi_1-\varphi_2)^2$$

und für $\frac{1}{2}J$ den Ausdruck

$$(\alpha-a)z_1^2+(b-\beta)z_1z_2+(a\beta-b\alpha)z_2^2.$$

Auch hier erkennt man sofort die Gültigkeit des Satzes.

§ 442. Wir wollen jetzt noch einige, die Functionaldeterminanten betreffende Sätze ableiten. Sind $(m+1)$ Gleichungen $f_\alpha=0$ in m Unbekannten $z_1,\cdots z_m$ gegeben, so können wir sie durch die Einführung einer neuen Variablen z_{m+1} unter Beibehaltung der Dimensionen n_α homogen machen. So entsteht das System

$$g_\alpha(z_1,z_2,\cdots z_m,z_{m+1})=0\qquad(\alpha=1,2,\cdots m+1).\tag{7}$$

Da nun nach dem Euler'schen Satze über homogene Functionen

$$z_1\frac{\partial g_\alpha}{\partial z_1}+z_2\frac{\partial g_\alpha}{\partial z_2}+\cdots+z_{m+1}\frac{\partial g_\alpha}{\partial z_{m+1}}=n_\alpha\cdot g_\alpha\tag{8}$$
$$(\alpha=1,2,\cdots m+1),$$

so wird jedes System $\zeta_1,\zeta_2,\cdots\zeta_{m+1}$, welches alle g_α zu Null macht, die in $z_1,z_2,\cdots z_{m+1}$ linearen Gleichungen (8) befriedigen, wenn die

rechten Seiten $=0$ gesetzt werden. Ist nun $(\zeta_1, \zeta_2, \cdots \zeta_{m+1}) \neq (0, 0, \cdots 0)$, dann muss durch die ζ die Determinante der linken Seiten

$$J = \frac{\partial(g_1, \cdots g_{m+1})}{\partial(\zeta_1, \cdots \zeta_{m+1})} = 0$$

werden, d. h. die Functionaldeterminante homogener Gleichungen mit ebensovielen Unbekannten verschwindet für jede von $(0, 0, \cdots 0)$ verschiedene Wurzel des Gleichungssystems.

§ 443. Die Form von J lehrt noch eine weitere Eigenschaft der Functionaldeterminante. Wir addiren zu der mit z_1 multiplicirten ersten Spalte von J die zweite mit z_2 multiplicirte u. s. w. bis zu der $(m+1)^{\text{ten}}$ mit z_{m+1} multiplicirten und wenden den Euler'schen Satz über homogene Functionen an. Dabei zeigt es sich: Das Product aus der Functionaldeterminante in eine beliebige der Variablen ist bei homogenen Functionen congruent Null nach dem aus den Functionen gebildeten Modulsysteme.

Die Darstellung der Functionaldeterminante homogener Functionen kann noch von einer anderen Seite her in Angriff genommen werden. Ist das System (7) vorgelegt, und sind $n_1, n_2, \cdots$ wie gewöhnlich die Dimensionen der Gleichungen, dann ist J von der Dimension $(n_1 + n_2 + \cdots + n_{m+1} - m - 1)$. Nach § 420 können wir nun Functionen $P_1, P_2, \cdots P_{m+1}$ so bestimmen, dass

$$(9) \qquad J - P_1 \cdot g_1 - P_2 \cdot g_2 - \cdots - P_{m+1} g_{m+1}$$

in z_1 höchstens bis zur Dimension $(n_1 - 1)$, in z_2 höchstens bis zur Dimension $(n_2 - 1), \cdots$ aufsteigt. Dabei sind freilich die Functionen P nicht sofort als homogen durch den angeführten Satz zu erkennen. Behält man jedoch aus etwaigen allgemeineren P je nur die Glieder höchster Dimension bei, so wird der Ausdruck (9) eine homogene Function der gleichen Eigenschaft. Es giebt aber nur das eine Potenzproduct $z_1^{n_1-1} z_2^{n_2-1} \cdots z_{m+1}^{n_{m+1}-1}$, welches den Gradbedingungen genügt. Folglich ist (9) gleich diesem Potenzproducte, multiplicirt mit einer Constanten.

Gesetzt, die Gleichungen (7) hätten eine von $(0, 0, \cdots 0)$ verschiedene Wurzel $(\zeta_1, \zeta_2, \cdots)$, dann wird für sie $J = 0$ und $g_1 = 0$, $g_2 = 0, \cdots g_{m+1} = 0$, also auch jene Constante $= 0$. Eine solche Wurzel besteht nur, wenn die Resultante der Gleichungen verschwindet. Demnach ist die Constante durch die Resultante R der Gleichungen theilbar, und es wird

$$(10) \qquad J = P_1 g_1 + \cdots + P_{m+1} g_{m+1} + c_1 R \cdot (z_1^{n_1-1} \cdots z_{m+1}^{n_{m+1}-1}).$$

Die letzten Schlüsse werden hinfällig, wenn eine der Coordinaten ζ gleich Null ist; aber gerade dann ist die letzte Gleichung selbstverständlich. So sind wir zu dem Satze gelangt: Stets dann und nur dann, wenn $R = 0$ ist, kann

$$J = P_1 g_1 + P_2 g_2 + \cdots + P_{m+1} g_{m+1} \tag{11}$$

gesetzt werden. Es ist also die Darstellungsmöglichkeit (11) charakteristisch dafür, dass die homogenen Gleichungen (7) eine von $(0, 0, \cdots 0)$ verschiedene Wurzel besitzen.

Wir wollen diesen Satz durch zwei Beispiele erläutern. Ist

$$g_1 = az_1^2 + 2bz_1z_2 + cz_2^2, \quad g_2 = \alpha z_1 + \beta z_2,$$

so wird

$$\begin{aligned}\frac{1}{2} J &= (a\beta - b\alpha)z_1 + (b\beta - c\alpha)z_2 \\ &= \frac{1}{\alpha}[(a\beta - b\alpha)g_2 - (a\beta^2 - 2b\alpha\beta + c\alpha^2)z_2],\end{aligned}$$

und hier ist der Coefficient von z_2 gleich der Resultante der Functionen

$$f_1 = at^2 + 2bt + c, \quad f_2 = \alpha t + \beta.$$

Ist zweitens

$$g_1 = az_1^2 + 2bz_1z_2 + cz_2^2, \quad g_2 = \alpha z_1^2 + 2\beta z_1 z_2 + \gamma z_2^2,$$

so wird

$$\frac{1}{2} J = 2(a\beta - b\alpha)z_1^2 + 2(a\gamma - c\alpha)z_1z_2 + 2(b\gamma - c\beta)z_2^2.$$

Setzt man dies $= pg_1 + qg_2$, wobei p und q Constanten bedeuten, dann wird durch Auflösung der Bedingungsgleichungen

$$p = 2\beta - \alpha\frac{a\gamma - c\alpha}{a\beta - b\alpha}, \quad q = -2b + a\frac{a\gamma - c\alpha}{a\beta - b\alpha},$$

aber auch

$$p = 2\beta - 4\alpha\frac{b\gamma - c\beta}{a\gamma - c\alpha}, \quad q = -2b - 4a\frac{b\gamma - c\beta}{a\gamma - c\alpha}.$$

Diese beiden Werthepaare stimmen hierbei nur dann überein, wenn

$$(a\gamma - c\alpha)^2 - 4(a\beta - b\alpha)(b\gamma - c\beta) = 0$$

ist, wie dies nach dem ausgesprochenen Satze sein muss, da der Ausdruck auf der linken Seite der Gleichung die Resultante aus

$$at^2 + 2bt + c = 0, \quad \alpha t^2 + 2\beta t + \gamma = 0$$

ist.

§ 444. Jacobi hat (l. c. § 3) ein System von q Gleichungen mit m Variablen als ein solches von untereinander unabhängigen Gleichungen definirt, wenn keine derselben identisch erfüllt ist oder mit Hülfe der übrigen zu einer identisch erfüllten gemacht werden kann. Um ein System auf seine Unabhängigkeit hin zu prüfen, wird

aus einer ersten Gleichung $f_1 = 0$ eine Unbekannte z_1 bestimmt; der erhaltene Werth in die anderen eingetragen und nachgesehen, ob dabei eine identisch erfüllte Gleichung entsteht. Ist dies nicht der Fall, so wird aus einer der neuen Gleichungen z_2 bestimmt; der erhaltene Werth wird in die anderen eingetragen u. s. f. Kommt man bei der Fortsetzung dieses Verfahrens auf keine identisch erfüllte Gleichung, dann heisst das System unabhängig. Hierbei sieht man zugleich, dass in diesem Falle ebensoviele Unbekannte bestimmt werden können, als Gleichungen vorhanden sind, während im Falle der Abhängigkeit das nicht eintritt. Deshalb gestaltet Jacobi seine Definition auch noch folgendermassen um: Die Gleichungen $f_1 = 0,\ f_2 = 0, \cdots f_q = 0$ heissen unabhängig oder abhängig von einander, jenachdem es möglich oder unmöglich ist, aus ihnen q Unbekannte zu bestimmen. Da es nun nicht angeht, mehr als q Unbekannte aus den q Gleichungen zu bestimmen, so folgt, dass die Anzahl unabhängiger Gleichungen nicht grösser sein kann als die Anzahl der eingehenden Unbekannten. —

Man sieht leicht ein, dass diese Jacobi'schen Definitionen strenger gefasst werden müssen. Will man sie z. B. auf die beiden Gleichungen

$$z_1(z_1 + z_2 - 3) = 0, \quad z_1(z_1 - z_2 - 1) = 0$$

anwenden, dann giebt der aus der ersten entnommene Werth $z_1 = 0$ für die zweite Gleichung eine identisch erfüllte; dagegen $z_1 = 3 - z_2$ nicht. Nach der ersten Definition könnten die Gleichungen wohl abhängig genannt werden, nach der zweiten wohl nicht.

Es scheint naturgemässer, zu definiren: $f_q = 0$ ist von $f_1 = 0, \cdots f_{q-1} = 0$ dann und nur dann abhängig, wenn jede Wurzel des Systems $f_1 = 0, \cdots f_{q-1} = 0$ auch die Gleichung $f_q = 0$ (abgesehen von der Multiplicität) befriedigt. Oder auch: $f_q = 0$ ist von $f_1 = 0, \cdots f_{q-1} = 0$ abhängig, wenn die Gesammteliminante der letzten $(q-1)$ Gleichungen mit der aller q Gleichungen identisch ist.

§ 445. Zum Schlusse dieser Vorlesung wollen wir noch ein mit den soeben behandelten Fragen verwandtes Problem untersuchen: Welche Gleichungen von der Form

$$(12)\quad f_1(z_1, \cdots z_m) P_1(z_1, \cdots z_m) + \cdots + f_q(z_1, \cdots z_m) P_q(z_1, \cdots z_m) = 0$$

können zwischen allgemeinen Functionen $f_1, f_2, \cdots f_q$ bestehen? Vgl. § 413 u. § 416.

Zunächst sei $q = 2$. Dann folgt aus

$$f_1 P_1 + f_2 P_2 = 0,$$

dass die allgemeine Function f_1 das Product $f_2 P_2$ und daher auch P_2 theilen muss. Setzt man nun $P_2 = -f_1 \cdot Q$, dann folgt $P_1 = f_2 \cdot Q$, so dass nur identische Gleichungen von der Form

$$f_1(f_2 Q) + f_2(-f_1 Q) = 0$$

möglich sind. Das Gleiche gilt auch bei besonderen Functionen f_1 und f_2, sobald nur beide keinen Factor gemeinsam besitzen.

Es sei ferner $q = 3$, so dass

$$f_1 P_1 + f_2 P_2 + f_3 P_3 = 0$$

zu erfüllen ist. Aus den drei f eliminiren wir z_1, z_2 und erhalten als Eliminante $R(z_3, z_4, \cdots z_m)$. Aus der Annahme, dass die f allgemeine Functionen sind, folgt, dass R nicht identisch verschwindet. Unsere folgenden Schlüsse gelten auch für jeden besonderen Fall, in welchem R nicht identisch Null ist, also für willkürliche Wahl von $z_3, z_4, \cdots z_m$ nicht unendlich viele Wurzeln für $f_1 = 0$, $f_2 = 0$, $f_3 = 0$ vorhanden sind.

Für jedes System $z_1, z_2, \ldots$, welches die beiden Gleichungen $f_1 = 0$, $f_2 = 0$ erfüllt, dagegen $f_3 \neq 0$ macht, muss $P_3 = 0$ werden; für jedes System $z_1, z_2, \cdots$, welches die drei Gleichungen $f_1 = 0$, $f_2 = 0$, $f_3 = 0$ erfüllt, muss $R = 0$ werden. Folglich verschwindet $P_3 \cdot R$ für alle Systeme $z_1, z_2, \cdots$, welche $f_1 = 0$, $f_2 = 0$ machen, gleichgültig, wie sich f_3 ihnen gegenüber verhält. Man hat also nach § 428, da bei allgemeinen Gleichungen nur einfache Wurzeln vorkommen,

$$P_3(z_1, z_2, z_3, \cdots) \cdot R(z_3, \cdots) = \varphi_1 f_1 + \varphi_2 f_2$$

und deswegen nach § 431 auch schon

$$P_3(z_1, z_2, z_3, \cdots) = Q_2 \cdot f_1 - Q_1 \cdot f_2 .$$

Daraus folgt dann

$$f_1(P_1 + Q_2 f_3) + f_2(P_2 - Q_1 f_3) = 0,$$

und also nach dem Resultate für $q = 2$

$$P_1 = Q_3 f_2 - Q_2 f_3, \quad P_2 = Q_1 f_3 - Q_3 f_1 .$$

Die geforderte Relation nimmt somit die Gestalt an

$$f_1(f_2 Q_3 - f_3 Q_2) + f_2(f_3 Q_1 - f_1 Q_3) + f_3(f_1 Q_2 - f_2 Q_1) = 0,$$

d. h. es ist eine identisch verschwindende Gleichung.

Setzt man diese Betrachtungen fort, so gelangt man zu dem allgemeinen Resultate: Die Gleichung (12) kann nur für Functionen

$$P_\alpha = Q_{\alpha 1} f_1 + Q_{\alpha 2} f_2 + \cdots + Q_{\alpha q} f_q$$

stattfinden, wobei die Q die Bedingungen

$$Q_{\alpha\beta} + Q_{\beta\alpha} = 0, \quad Q_{\alpha\alpha} = 0$$

zu erfüllen haben, sonst aber beliebig gewählt werden dürfen.

§ 446. In ähnlicher Art behandeln wir die Frage: Welche Gleichungen von der Form

$$(13)\qquad f_1 f_2 \cdot P_{1,2} + f_1 f_3 \cdot P_{1,3} + \cdots + f_{q-1} f_q \cdot P_{q-1,q} = 0$$

können zwischen allgemeinen Functionen $f_1, f_2, \cdots f_q$ bestehen? Zunächst sei $q = 3$; dann folgt aus

$$f_1(f_2 P_{1,2} + f_3 P_{1,3}) + f_2\,(f_3 P_{2,3}) = 0$$

nach dem vorigen Paragraphen, dass $P_{2,3}$ durch f_1 theilbar ist und ebenso weiter, so dass wir setzen können

$$P_{1,2} = Q' f_3,\quad P_{1,3} = Q'' f_2,\quad P_{2,3} = Q''' f_1,$$

sobald die f allgemeine Functionen sind, ja auch schon, wenn sie keinen Factor gemeinsam haben. Setzt man diese Resultate ein, so folgt als Bedingungsgleichung

$$Q' + Q'' + Q''' = 0.$$

Bei $q = 4$ ordnen wir die Gleichung folgendermassen:

$$(13^a)\quad f_1[f_2 P_{1,2} + f_3 P_{1,3} + f_4 P_{1,4}] + f_2[f_3 P_{2,3} + f_4 P_{2,4}] + f_3 f_4 P_{3,4} = 0.$$

Genau derselbe Schluss wie im vorigen Paragraphen zeigt uns, dass bei der Elimination von z_1 und z_2 zwischen f_1, f_2 und $f_3 f_4$ das Product $P_{3,4} \cdot R(f_1, f_2, f_3 f_4)$ und dann auch $P_{3,4}$ durch f_1 und f_2 homogen und linear darstellbar ist; das Entsprechende gilt von allen $P_{\alpha\beta}$. Daher ist

$$P_{1,4} = Q_{1,4,2} f_2 + Q_{1,4,3} f_3;\quad P_{2,4} = Q_{2,4,1} f_1 + Q_{2,4,3} f_3;$$
$$P_{3,4} = Q_{3,4,1} f_1 + Q_{3,4,2} f_2.$$

Tragen wir dies in die Gleichung (13^a) ein, dann ist die Frage auf $q = 3$ reducirt, und wir erkennen, dass

$$P_{\alpha\beta} = Q_{\alpha\beta\gamma} f_\gamma + Q_{\alpha\beta\delta} f_\delta;$$
$$Q_{\alpha\beta\gamma} + Q_{\beta\gamma\alpha} + Q_{\gamma\alpha\beta} = 0;\quad Q_{\alpha\beta\gamma} = Q_{\beta\alpha\gamma}$$

zu setzen ist, wobei ausser den angegebenen beiden Beschränkungen für die Q keine anderen bestehen.

Dieselbe Methode führt auf das allgemeine Resultat: Sind f_1, $f_2, \cdots f_q$ allgemeine Functionen, dann kann (13) nur statt, finden, wenn jedes

$$P_{\alpha\beta} = Q_{\alpha\beta\gamma} f_\gamma + Q_{\alpha\beta\delta} f_\delta + \cdots + Q_{\alpha\beta q} f_q$$

ist, wobei die Q bis auf die Beschränkungen

$$Q_{\alpha\beta\gamma} + Q_{\beta\gamma\alpha} + Q_{\gamma\alpha\beta} = 0;\quad Q_{\alpha\beta\gamma} = Q_{\beta\alpha\gamma}$$

ganz willkürlich gewählt werden können.

Man erkennt leicht, dass den Problemen dieses und des vorigen Paragraphen ähnliche in derselben Richtung zur Seite stehen, und man sieht auch, wie die Lösung sich gestalten wird.

Dreiundvierzigste Vorlesung.

Die Cayley'sche und die Sylvester'sche Eliminationsmethode.

§ 447. In § 139 (Bd. I) haben wir die Resultante zweier Gleichungen $f(z) = 0$ vom m^{ten} und $g(z) = 0$ vom n^{ten} Grade in der Form einer Determinante dargestellt, indem wir die $(m + n - 1)$ Potenzen $z, z^2, \cdots z^{m+n-1}$ aus den $(m + n)$ Gleichungen

$$f = 0,\ z \cdot f = 0, \cdots z^{n-1} \cdot f = 0;\ g = 0,\ z \cdot g = 0, \cdots z^{m-1} \cdot g = 0$$

eliminirten.

Sind mehrere Gleichungen mit mehreren Unbekannten gegeben, dann liegen die Verhältnisse insofern complicirter, als bei ähnlichem Vorgehen die Anzahl der zu eliminirenden Potenzproducte nicht mit der Anzahl der Gleichungen übereinstimmt. Bei hinreichend hoher Dimension der Potenzproducte wird die Anzahl der Gleichungen die grössere. Cayley hat diese Verhältnisse genauer studirt*). Wir müssen uns damit begnügen, seine Untersuchungen kurz zu erwähnen, da seine Schlüsse nicht immer bindend und seine Hülfssätze zum Theil unrichtig sind. Ob seine Resultate dadurch beeinflusst werden, mag dahingestellt bleiben.

Wir gehen von $(m + 1)$ Gleichungen mit m Unbekannten aus

$$(1) \qquad f_\alpha(z_1, z_2, \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots m + 1);$$

dabei habe f_α die Dimension n_α. Die Coefficienten der Function f_α sollen generell mit c_α und diejenigen eines unterschiedlos gewählten f mit c bezeichnet werden. Die f sollen allgemeine vollständige Functionen sein. Nun multipliciren wir jedes f_α mit jedem Gliede

$$1;\ z_1, z_2, \cdots z_m;\ z_1^2,\ z_1 z_2, \cdots z_m^2; \cdots,$$

so weit, bis die Multiplication von f_α mit den Potenzproducten zu allen Ausdrücken der Dimension n geführt hat, wobei n eine noch zu bestimmende Zahl bedeutet. Wir bekommen dadurch nach § 334

$$\sum_{\alpha=1}^{m+1} N(n - n_\alpha, m) = \Sigma_1$$

Gleichungen, die wir durch $u_1 = 0$, $u_2 = 0$, $u_3 = 0, \cdots$ bezeichnen wollen. Die Functionen u steigen nur bis zur Dimension n hinauf; es kommen demnach nur $N(n, m) = N$ verschiedene Potenzproducte der m Unbekannten vor.

*) On the theory of involution in Geometry. Cambr. a. Dubl. math. J. 2 (1847), p. 52; On the theory of Elimination; ibid. 3 (1848), p. 116.

Es handelt sich nun zunächst um die Beantwortung der Frage, ob man n so gross wählen kann, dass die Anzahl der Gleichungen gleich oder grösser wird als die Anzahl der Potenzproducte der Unbekannten. Abgesehen von dem, beiden Zahlen gemeinsamen Nenner $m!$ liefert die Entwickelung unserer Ausdrücke nach fallenden Potenzen von n die Anfangsglieder

$$(m+1)n^m - \cdots \quad \text{und} \quad n^m + \cdots.$$

Daraus folgt sofort die Möglichkeit der Bestimmung. Für die genauere Feststellung des n haben wir bereits in § 335 die nothwendigen Voruntersuchungen gemacht. Setzen wir

$$n = n_1 + n_2 + \cdots + n_{m+1} - m, \tag{2}$$

dann ist die Voraussetzung der dort gegebenen Formel (14) erfüllt, und wir haben

$$\Sigma_1 > N.$$

Es reicht also aus, n gemäss (2) zu wählen, um ein System von Gleichungen zu erhalten, deren Anzahl diejenige der in ihnen auftretenden verschiedenen Potenzproducte der m Unbekannten $z_1, z_2, \cdots z_m$ übertrifft.

§ **448.** Nehmen wir jetzt aus den Σ_1 so erhaltenen Gleichungen irgend welche N Gleichungen heraus und bilden die Determinante Δ der Coefficienten aller Potenzproducte inclusive $z_1^0 z_2^0 \cdots z_m^0$, dann muss Δ verschwinden, sobald $(z_1, z_2, \cdots z_m)$ so gewählt werden kann, dass die $(m+1)$ Gleichungen (1) und mit ihnen die Σ_1 Gleichungen $u_1 = 0$, $u_2 = 0, \cdots$ befriedigt sind.

Verfährt man mit Δ genau so, wie es in § 149, Bd. I mit der für zwei Gleichungen einer Unbekannten ähnlich gebildeten Determinante geschehen ist, indem wir jede Spalte mit demjenigen Potenzproducte der Unbekannten multipliciren, zu dessen Coefficienten gerade die Elemente dieser Spalte gehörten, und diese Producte dann sämmtlich zu den Elementen derjenigen Spalte addiren, die dem Potenzproducte $z_1^0 z_2^0 \cdots z_m^0 = 1$ zuzuordnen ist, dann entsteht, genau wie dort,

$$\Delta = f_1 M_1 + f_2 M_2 + \cdots + f_{m+1} M_{m+1}, \tag{3}$$

wobei M_α höchstens bis zur Dimension $(n - n_\alpha)$ aufsteigen kann.

Wir müssen nun die beiden Möglichkeiten in Betracht ziehen, dass entweder $\Delta \equiv 0$ ist, oder dass Δ nicht identisch verschwindet.

Im zweiten Falle erkennen wir aus dem Umstande, dass Δ für jedes Coefficientensystem der c verschwindet, welches die Resultante R von (1) befriedigt, nach § 346, IX und § 390 die Richtigkeit des Satzes: Die Determinante Δ ist, falls sie nicht identisch verschwindet, ein Multiplum der Resultante R der Gleichungen (1).

Es handelt sich nun um die Frage, wann Δ in (3) identisch verschwinden kann. Nach den Erörterungen am Schlusse der letzten Vorlesung ist dies nur dann möglich, wenn jedes M_α linear und homogen in $f_1, f_2, \cdots f_{\alpha-1}, f_{\alpha+1}, \cdots f_{m+1}$ gewählt wird. Man erhält demgemäss sämmtliche Gleichungen

$$(4) \qquad 0 = f_1 M_1 + f_2 M_2 + \cdots + f_{m+1} M_{m+1},$$

wenn wir alle möglichen

$$(5) \qquad f_\alpha (Q_{\alpha\beta} f_\beta) - f_\beta (Q_{\alpha\beta} f_\alpha) = 0 \qquad (\alpha, \beta = 1, 2, \cdots m+1;\ \alpha \neq \beta)$$

bilden, worin $Q_{\alpha\beta}$ nur bis zur Dimension $(n - n_\alpha - n_\beta)$ aufsteigen darf, weil M_α die Dimension $(n - n_\alpha)$ nicht überschreitet, und wenn wir dann alle (5) linear combiniren. Man erhält daher so viele Relationen (5), als in allen $Q_{\alpha\beta}$ Potenzproducte vorkommen; d. h. es giebt

$$\sum_{\alpha, \beta} N(n - n_\alpha - n_\beta, m) = \Sigma_2$$

Relationen (5), aus denen sich alle Gleichungen (4) linear zusammensetzen lassen.

§ 449. Im Falle $m = 2$, d. h. bei drei Gleichungen zwischen z_1 und z_2 folgt auch leicht weiter, dass die Relationen (5) sämmtlich untereinander unabhängig sind. Denn nach § 446 können Relationen zwischen den $Q_{\alpha\beta} \cdot f_\alpha f_\beta$, $Q_{\alpha\gamma} \cdot f_\alpha f_\gamma$, $Q_{\beta\gamma} \cdot f_\beta f_\gamma$ nur auftreten, wenn jedes Q durch das noch fehlende f theilbar ist. Dann würden aber die Glieder dieser Relationen bis zu Dimensionen $(n_1 + n_2 + n_3)$ aufsteigen, was nach (2) ausgeschlossen ist. Da also unter den Σ_1 Gleichungen $u_1 = 0$, $u_2 = 0, \cdots$ hier Σ_2 und nur so viele unabhängige Relationen bestehen, muss $\Sigma_1 - \Sigma_2 = N$ sein, wie dies auch § 335 zeigt, und wie es sich auch leicht durch directe Rechnung gemäss der Gleichung

$$\begin{aligned}(n_1 + n_2 + n_3)(n_1 + n_2 + n_3 - 1) + n_1(n_1 - 1) + n_2(n_2 - 1) + n_3(n_3 - 1) \\ = (n_1 + n_2)(n_1 + n_2 - 1) + (n_1 + n_3)(n_1 + n_3 - 1) + (n_2 + n_3)(n_2 + n_3 - 1)\end{aligned}$$

ergiebt. Die Σ_2 Relationen (5) denken wir uns so geschrieben, dass alle $(Q_{\alpha\beta} f_\beta)$, $(Q_{\alpha\beta} f_\alpha)$ nach Potenzproducten $z_1^{\mu_1} z_2^{\mu_2} \cdots z_m^{\mu_m}$ geordnet werden; multiplicirt man dann mit diesen Potenzproducten in die f_α bezw. f_β, dann bekommt man alle Relationen $v_1 = 0$, $v_2 = 0, \cdots$, welche zwischen den $z_1^{\mu_1} z_2^{\mu_2} \cdots f_\alpha$ bestehen, d. h. zwischen den $u_1 = 0$, $u_2 = 0, \cdots$.

Im Falle $m = 3$, also bei vier Gleichungen zwischen z_1, z_2, z_3 sind die eben gebildeten $v_1 = 0$, $v_2 = 0, \cdots$ nicht alle von einander unabhängig; es ist nach § 335, (14) nämlich $\Sigma_1 - \Sigma_2 < N$. In der That können hier auch zwischen den $Q_{\alpha\beta} f_\alpha f_\beta$ in Formel (5) nach den Darlegungen von § 446 Relationen von der Form

$$(Q_{\alpha\beta\gamma} f_\gamma) \cdot f_\alpha f_\beta = (Q_{\alpha\beta\gamma} f_\beta) \cdot f_\alpha f_\gamma = (Q_{\alpha\beta\gamma} f_\alpha) \cdot f_\beta f_\gamma$$

auftreten, wobei $Q_{\alpha\beta\gamma}$ bis zur Dimension $(n - n_\alpha - n_\beta - n_\gamma)$ aufsteigen darf und sonst ganz beliebig ist. Diese Relationen wollen wir durch $w_1 = 0$, $w_2 = 0, \cdots$ bezeichnen. Ihre Anzahl beträgt

$$\sum_{\alpha,\beta,\gamma} N(n - n_\alpha - n_\beta - n_\gamma, 3) = \Sigma_3,$$

und da nach § 335, (14) bei $m = 3$

$$N = \Sigma_1 - \Sigma_2 + \Sigma_3$$

ist, so lässt sich vermuthen, dass die w voneinander unabhängig sind. Dies folgt auch wirklich aus den Resultaten von § 446. —

In gleicher Weise können wir für $m = 4$ vorgehen; doch reicht es aus, wenn wir hier stehen bleiben.

Cayley giebt nun ohne Beweis folgendes Resultat an: Die Coefficienten der u werden in einem Rechtecke Q_1 von N Spalten und Σ_1 Zeilen angeordnet, so dass die Coefficienten eines jeden u je eine Zeile füllen. — Dahinter werden die Coefficienten der v in einem Rechtecke Q_2 von Σ_1 Zeilen und Σ_2 Spalten angeordnet, so dass die Coefficienten eines jeden v je eine Spalte füllen, und die Elemente jeder Zeile demselben u entsprechen, dem diese Zeile in Q_1 angehört. — Unter Q_2 werden die Coefficienten der w in einem Rechtecke Q_3 von Σ_2 Spalten und Σ_3 Zeilen angeordnet, so dass die Coefficienten eines jeden w je eine Zeile füllen, und die Elemente jeder Spalte dem v entsprechen, dem diese Spalte in Q_2 angehört.

Q_1	Q_2
Coeffic. der u	Coeffic. der v
Σ_1 Zeilen	Σ_1 Zeilen
N Spalten	Σ_2 Spalten
	Q_3
	Coeffic. der w
	Σ_2 Spalten
	Σ_3 Zeilen

$$N = \Sigma_1 - \Sigma_2 + \Sigma_3.$$

Aus Q_3 wählt man eine nicht identisch verschwindende Determinante Δ_3 der Ordnung Σ_3; aus den, den nicht benutzten entsprechenden Spalten von Q_2 eine nicht identisch verschwindende Determinante Δ_2 der Ordnung $(\Sigma_2 - \Sigma_3)$; und aus den, den nicht benutzten entsprechenden Zeilen von Q_1 eine Determinante Δ_1 der Ordnung $[\Sigma_1 - (\Sigma_2 - \Sigma_3)] = N$. Dann ist

$$\frac{\Delta_1 \Delta_3}{\Delta_2} = 0$$

die charakteristische Bedingung dafür, dass die u eine gemeinsame Wurzel haben. Der Quotient $(\Delta_1 \Delta_3) : \Delta_2$ hat als Dimension in den Coefficienten

$$[\Sigma_1 - (\Sigma_2 - \Sigma_3)] - [\Sigma_2 - \Sigma_3] + \Sigma_3 = \Sigma_1 - 2\Sigma_2 + 3\Sigma_3,$$

also nach § 336, (15)

$$= n_1 n_2 + n_2 n_3 + n_3 n_1,$$

so dass er mit der Resultante von (1) übereinstimmt. —

Für $m > 3$ tritt hinter Q_3 noch ein Q_4, unter Q_4 noch ein Q_5 u. s. f. Die Möglichkeit der Determinantenbildung wird dadurch gewährleistet, dass nach § 335, (14)

$$N = \Sigma_1 - \Sigma_2 + \Sigma_3 - \cdots$$

wird; so kann man Determinanten der Ordnungen

$$\Sigma_1 - \Sigma_2 + \Sigma_3 - \cdots; \; \Sigma_2 - \Sigma_3 + \cdots; \; \Sigma_3 - \cdots$$

bilden. Nach Cayley soll der Quotient

$$\text{(6)} \qquad \frac{\Delta_1 \Delta_3 \Delta_5 \cdots}{\Delta_2 \Delta_4 \Delta_6 \cdots}$$

durch sein Verschwinden die charakteristische Bedingung für die Erfüllbarkeit der $u = 0$, d. h. der $f_\alpha = 0$ liefern; und da die Dimension des Ausdrucks (6) gleich derjenigen der Resultante

$$[\Sigma_1 - \Sigma_2 + \Sigma_3 - \cdots] - [\Sigma_2 - \Sigma_3 + \cdots] + [\Sigma_3 - \cdots] - \cdots$$
$$= \Sigma_1 - 2\Sigma_2 + 3\Sigma_3 - \cdots = n_1 n_2 n_3 \cdots \left(\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \cdots\right)$$

ist, so würde (6) mit der Resultante R übereinstimmen.

Wir wollen hier das von Cayley (On the theory of elimination) gegebene einfache Beispiel für $m = 2$; $n_1 = n_2 = n_3 = 2$ und also $n = 4$ nachfolgen lassen:

$$f_1 = a_1 + b_1 z_1 + c_1 z_2 + d_1 z_1^2 + e_1 z_1 z_2 + g_1 z_2^2 = 0,$$
$$f_2 = a_2 + b_2 z_1 + c_2 z_2 + d_2 z_1^2 + e_2 z_1 z_2 + g_2 z_2^2 = 0,$$
$$f_3 = a_3 + b_3 z_1 + c_3 z_2 + d_3 z_1^2 + e_3 z_1 z_2 + g_3 z_2^2 = 0.$$

Die f sind der Reihe nach mit 1; z_1, z_2; $z_1^2, z_1 z_2, z_2^2$ zu multipliciren. So entstehen 18 Ausdrücke u

$$f_1 = u_1' \; ; \; z_1 f_1 = u_2' \; , \; z_2 f_1 = u_3' \; ; \; z_1^2 f_1 = u_4' \; , \; z_1 z_2 f_1 = u_5' \; , \; z_2^2 f_1 = u_6' \; ;$$
$$f_2 = u_1'' \; ; \; z_1 f_2 = u_2'' , \; z_2 f_2 = u_3'' ; \; z_1^2 f_2 = u_4'' , \; z_1 z_2 f_2 = u_5'' , \; z_2^2 f_2 = u_6'' ;$$
$$f_3 = u_1''' ; \; z_1 f_3 = u_2''' , \; z_2 f_3 = u_3''' ; \; z_1^2 f_3 = u_4''' , \; z_1 z_2 f_3 = u_5''' , \; z_2^2 f_3 = u_6''' .$$

Zwischen den u bestehen wegen $f_\alpha f_\beta - f_\beta f_\alpha = 0$ folgende drei Relationen:

$$
\begin{aligned}
&a_2 u_1' + b_2 u_2' + c_2 u_3' + d_2 u_4' + e_2 u_5' + g_2 u_6' \\
&\qquad - a_1 u_1'' - b_1 u_2'' - c_1 u_3'' - d_1 u_4'' - e_1 u_5'' - g_1 u_6'' = 0, \\
&- a_3 u_1' - b_3 u_2' - c_3 u_3' - d_3 u_4' - e_3 u_5' - g_3 u_6' \\
&\qquad + a_1 u_1''' + b_1 u_2''' + c_1 u_3''' + d_1 u_4''' + e_1 u_5''' + g_1 u_6''' = 0, \\
&a_3 u_1'' + b_3 u_2'' + c_3 u_3'' + d_3 u_4'' + e_3 u_5'' + g_3 u_6'' \\
&\qquad - a_2 u_1''' - b_2 u_2''' - c_2 u_3''' - d_2 u_4''' - e_2 u_5''' - g_2 u_6''' = 0.
\end{aligned}
$$

Aus diesen Gleichungen setzen sich Q_1 und Q_2 zusammen:

$$
\begin{array}{ccccccccccccccc|ccc}
a_1 & b_1 & c_1 & d_1 & e_1 & g_1 & & & & & & & & & & a_2 & -a_3 & \\
 & a_1 & & b_1 & c_1 & & d_1 & e_1 & g_1 & & & & & & & b_2 & -b_3 & \\
 & & a_1 & & b_1 & c_1 & & d_1 & e_1 & g_1 & & & & & & c_2 & -c_3 & \\
 & & & a_1 & & & b_1 & c_1 & & & d_1 & e_1 & g_1 & & & d_2 & -d_3 & \\
 & & & & a_1 & & & b_1 & c_1 & & & d_1 & e_1 & g_1 & & e_2 & -e_3 & \\
 & & & & & a_1 & & & b_1 & c_1 & & & d_1 & e_1 & g_1 & g_2 & -g_3 & \\
a_2 & b_2 & c_2 & d_2 & e_2 & g_2 & & & & & & & & & & -a_1 & & a_3 \\
 & a_2 & & b_2 & c_2 & & d_2 & e_2 & g_2 & & & & & & & -b_1 & & b_3 \\
 & & a_2 & & b_2 & c_2 & & d_2 & e_2 & g_2 & & & & & & -c_1 & & c_3 \\
 & & & a_2 & & & b_2 & c_2 & & & d_2 & e_2 & g_2 & & & -d_1 & & d_3 \\
 & & & & a_2 & & & b_2 & c_2 & & & d_2 & e_2 & g_2 & & -e_1 & & e_3 \\
 & & & & & a_2 & & & b_2 & c_2 & & & d_2 & e_2 & g_2 & -g_1 & & g_3 \\
a_3 & b_3 & c_3 & d_3 & e_3 & g_3 & & & & & & & & & & & a_1 & -a_2 \\
 & a_3 & & b_3 & c_3 & & d_3 & e_3 & g_3 & & & & & & & & b_1 & -b_2 \\
 & & a_3 & & b_3 & c_3 & & d_3 & e_3 & g_3 & & & & & & & c_1 & -c_2 \\
 & & & a_3 & & & b_3 & c_3 & & & d_3 & e_3 & g_3 & & & & d_1 & -d_2 \\
 & & & & a_3 & & & b_3 & c_3 & & & d_3 & e_3 & g_3 & & & e_1 & -e_2 \\
 & & & & & a_3 & & & b_3 & c_3 & & & d_3 & e_3 & g_3 & & g_1 & -g_2
\end{array}
$$

Die Resultante R wird gefunden, indem man aus den letzten drei Spalten eine der nicht identisch verschwindenden Determinanten Δ_2 bildet; das ist auf mancherlei Arten möglich. Aus den hierbei nicht benutzten Zeilen der ersten 15 Spalten wird die zweite Determinante Δ_1 gebildet; diese ist durch jene theilbar, und der Quotient $\Delta_1 : \Delta_2$ giebt bis auf einen constanten Factor die Resultante der drei Gleichungen $f_1 = 0$, $f_2 = 0$, $f_3 = 0$.

§ 450. Zum Zwecke des Beweises fasst Cayley das Problem allgemeiner. „Zwischen n Grössen $x_1, x_2, \cdots$ sind p $(> n)$ homogene lineare Gleichungen gegeben, $u_1 = 0$, $u_2 = 0, \cdots$; zwischen diesen bestehen $q = p - n$ lineare homogene Relationen. Die charakteristischen

Bedingungen dafür zu suchen, dass die $u = 0$ eine von $(0, 0, \cdots)$ verschiedene Wurzel haben"; dies ist die für $m = 2$ präcisirte Aufgabe. Wir wollen $n = 2$; $p = 4$, $q = 2$ nehmen, also etwa

$$u_1 \equiv a_{11}x_1 + a_{12}x_2 = 0, \cdots \quad u_4 \equiv a_{41}x_1 + a_{42}x_2 = 0;$$
$$v_1 \equiv b_{11}u_1 + \cdots + b_{14}u_4 = 0, \quad v_2 \equiv b_{21}u_1 + \cdots + b_{24}u_4 = 0.$$

Dann lässt sich leicht zeigen, dass

$$\frac{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}{\begin{vmatrix} b_{13} & b_{14} \\ b_{23} & b_{24} \end{vmatrix}} = -\frac{\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}}{\begin{vmatrix} b_{12} & b_{14} \\ b_{22} & b_{24} \end{vmatrix}} = \cdots = \frac{\begin{vmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{vmatrix}}{\begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix}} = \frac{\Delta_1}{\Delta_2}$$

ist. Nun behauptet Cayley und ebenso Salmon*), dass das Verschwinden dieses Quotienten die gesuchte Bedingung liefert. Das ist aber, wie aus einem Beispiel ersichtlich wird, unrichtig. Wir nehmen

$$u_1 \equiv t(t-2)x_1 + tx_2, \qquad u_2 \equiv t(3t-1)x_1 + tx_2,$$
$$u_3 \equiv t(-4t+3)x_1 - tx_2, \quad u_4 \equiv +5tx_1 + x_2,$$

wobei t einen beliebigen Parameter bedeutet. Dann gelten die Relationen zwischen den u

$$v_1 \equiv u_1 + (1+t)u_2 + (1+2t)u_3 + (-t+t^2)u_4 = 0,$$
$$v_2 \equiv (1+t)u_1 + (1-t)u_2 + (1+2t)u_3 + (-t+2t)^2 u_4 = 0,$$

und es wird der entscheidende Quotient

$$\frac{\Delta_1}{\Delta_2} = -1.$$

Es dürfte also das System $u_\alpha = 0$ nie befriedigt werden. Für $t = 0$ aber reicht $x_2 = 0$ bei beliebigem x_1 zur Befriedigung aus. Also schon in diesem einfachsten Falle versagt die Beweismethode.

Es ist klar, wie das allgemeine Problem lautet.

§ 451. J. J. Sylvester hat im Cambr. and Dubl. Math. J. 7 (1852), p. 68 „On the principles of the calculus of forms" eine andere Methode angegeben, mit deren Hülfe es gelingt, die Resultante von drei Gleichungen derselben Dimension in zwei Unbekannten als eine Determinante darzustellen.

Wir führen sie der Vollständigkeit halber hier an, trotzdem auch sie an Strenge der Beweisführung zu wünschen lässt.

Der Bequemlichkeit halber schreiben wir die drei Gleichungen als homogene Gleichungen dreier Unbekannten von n^{ter} Dimension

$$(7) \qquad f_1(z_1, z_2, z_3) = 0, \quad f_2(z_1, z_2, z_3) = 0, \quad f_3(z_1, z_2, z_3) = 0.$$

*) Lessons introduct. to the Modern Higher Algebra (4.) (1885), p. 88—89.

Es sei auf alle mögliche Weise die noch unbekannte positive Zahl k in drei ganze positive Summanden zerlegt

$$k = \alpha + \beta + \gamma.$$

Wenn dann jeder von diesen $\leqq n$ ist, dann kann man sicher

$$\begin{aligned} f_1 &= z_1^\alpha P'_\alpha + z_2^\beta Q'_\beta + z_3^\gamma R'_\gamma, \\ f_2 &= z_1^\alpha P''_\alpha + z_2^\beta Q''_\beta + z_3^\gamma R''_\gamma, \\ f_3 &= z_1^\alpha P'''_\alpha + z_2^\beta Q'''_\beta + z_3^\gamma R'''_\gamma \end{aligned}$$

ansetzen, wobei die P, Q, R ganze Functionen der Variablen bedeuten. Die Zerlegung von k kann auf $\frac{(k-1)(k-2)}{1 \cdot 2}$ verschiedene Arten vor sich gehen; für jede wählen wir eine solche Darstellung der f. Giebt es nun eine von $(0, 0, 0)$ verschiedene Wurzel $(\zeta_1, \zeta_2, \zeta_3)$ der drei Gleichungen (7), dann ist für diese die Determinante

$$D_{\alpha,\beta,\gamma} \equiv \begin{vmatrix} P'_\alpha & Q'_\beta & R'_\gamma \\ P''_\alpha & Q''_\beta & R'''_\gamma \\ P'''_\alpha & Q'''_\beta & R'''_\gamma \end{vmatrix} = 0.$$

Man erhält also hierdurch $\frac{(k-1)(k-2)}{1 \cdot 2}$ verschiedene Functionen

$$D_{\alpha\beta\gamma}(z_1, z_2, z_3), \tag{8}$$

welche homogen in den z_1, z_2, z_3 von der Dimension $(3n - k)$ sind und für $(\zeta_1, \zeta_2, \zeta_3)$ verschwinden.

Multipliciren wir ferner die drei $f(z_1, z_2, z_3)$ der Reihe nach mit allen Potenzproducten $z_1^\varkappa z_2^\lambda z_3^\mu$, in denen $\varkappa + \lambda + \mu = 2n - k$ ist, dann erhalten wir zu (8) noch weitere

$$3N(2n-k, 2) = \frac{3}{2}(2n - k + 2)(2n - k + 1)$$

homogene Gleichungen derselben Dimension $(3n - k)$. Wir haben damit also im Ganzen

$$\frac{1}{2}(k-2)(k-1) + \frac{3}{2}(2n - k + 2)(2n - k + 1)$$

Gleichungen zwischen

$$N(3n - k, 2) = \frac{1}{2}(3n - k + 2)(3n - k + 1)$$

Potenzproducten; diese Gleichungen werden für jede eigentliche Wurzel von (7) befriedigt. Setzt man nun die beiden letzten Anzahlen einander gleich, so entsteht zur Bestimmung von k die Gleichung

$$k^2 - (2n + 3)k + (n^2 + 3n + 2) = 0,$$

welche $k = n + 1$ oder $k = n + 2$ giebt. Damit ist auch die Bedingung befriedigt, dass keiner der Summanden α, β, γ grösser als n genommen

werden darf. Wir haben also die Möglichkeit, aus den vorhandenen Gleichungen sämmtliche Potenzproducte zu eliminiren. Dabei entsteht, weil jedes der $D_{\alpha\beta\gamma}$ in den Coefficienten der f von der Dimension 3 ist, eine Determinante von der Ordnung

$$3\cdot\frac{1}{2}(k-1)(k-2)+\frac{3}{2}(2n-k+2)(2n-k+1)$$
$$=3[k^2-(2n+3)k+(n^2+3n+2)]+3n^2=3n^2,$$

so dass die Determinante des Gleichungssystems nicht nur die Resultante enthält, sondern bis auf einen constanten Factor mit der Resultanten identisch ist.

Diese Sylvester'sche Methode versagt schon bei vier homogenen Gleichungen unbestimmter Dimension

$$f_1(z_1, z_2, z_3, z_4)=0, \cdots f_4(z_1, z_2, z_3, z_4)=0.$$

Verfährt man hier ähnlich wie oben, indem man

$$f_x = z_1^\alpha P_\alpha^{(x)} + z_2^\beta Q_\beta^{(x)} + z_3^\gamma R_\gamma^{(x)} + z_4^\delta S_\delta^{(x)}$$
$$(\alpha+\beta+\gamma+\delta=k)$$

setzt, und versucht man die Anzahl der Gleichungen derjenigen der Potenzproducte gleich zu machen, dann kommt man zur Bestimmung von k auf die Gleichung

$$N(4n-k, 3) = 4N(3n-k, 3) + (k-1)(k-2)(k-3);$$

diese liefert aber für unbestimmte n keine ganzzahligen positiven k als Wurzeln. Nur für $n=2$ erhält man $k=5$; dies heisst also, dass im Falle von vier quadratischen homogenen Formen, wie Sylvester auch angiebt, die Methode verwendbar bleibt.

Vierundvierzigste Vorlesung.

Discriminanten.

§ 452. Wir haben in § 158, Bd. I, die Bedingung dafür besprochen, dass eine Gleichung $f(z)=0$ mehrfache Wurzeln besitzt; sie bestand darin, dass ein gewisser aus den Coefficienten der Gleichung rational gebildeter Ausdruck, die Discriminante*), verschwindet.

Die hierauf führenden Betrachtungen können nach zweierlei Rich-

*) Es sei nachträglich bemerkt, dass diese Bezeichnung von Sylvester herrührt. Cambr. a. Dubl. M. J. 6 (1852), p. 52.

tungen auf das Gebiet mehrerer Variabeln ausgedehnt werden. Zunächst bietet sich die folgende Verallgemeinerung dar.

Ist ein System von m Gleichungen mit m Variablen

$$(1) \qquad f_\alpha(z_1, z_2, \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots m)$$

gegeben, welches nur eine endliche Anzahl von Wurzeln besitzt, so kann man dieselbe Frage aufwerfen: „welches ist die charakteristische Bedingung dafür, dass (1) mehrfache Wurzeln besitzt?" Führen wir wie früher nach Liouville statt z_m in (1) ein $x = \varkappa_1 z_1 + \cdots + \varkappa_{m-1} z_{m-1} + z_m$ und bilden dann die Eliminantengleichung $R(x) = 0$, so wird (1) dann und nur dann mehrfache Wurzeln haben, wenn $R(x) = 0$ solche besitzt. Die charakteristische Bedingung ist die, dass die Discriminante von $R(x)$ verschwindet. Dieser Ausdruck enthält die Parameter $\varkappa_1, \varkappa_2, \cdots$; es müssen also die einzelnen Coefficienten der Potenzproducte dieser Parameter, so weit sie in der Discriminante vorkommen, verschwinden.

Ist z. B. bei unbestimmten Coefficienten

$$f_1 \equiv a z_1^2 + 2b z_1 z_2 + c z_2^2 + 2d z_1 + 2e z_2 + g = 0,$$
$$f_2 \equiv \alpha z_1 + \beta z_2 + \gamma = 0,$$

und führen wir für z_2 ein $x - \varkappa z_1$, so ergiebt sich für die Eliminante

$$\begin{aligned} R(x) = {} & (a\beta^2 - 2b\alpha\beta + c\alpha^2)x^2 \\ & + 2[(a\beta\gamma - b\alpha\gamma - d\alpha\beta + e\alpha^2) - \varkappa(b\beta\gamma - c\alpha\gamma - d\beta^2 + e\alpha\beta)]x \\ & + [(a\gamma^2 - 2d\alpha\gamma + g\alpha^2) - 2\varkappa(b\gamma^2 - d\beta\gamma - e\alpha\gamma + g\alpha\beta) \\ & \quad + \varkappa^2(c\gamma^2 - 2e\beta\gamma + g\beta^2)]. \end{aligned}$$

Die Discriminante von R lässt sich auf die Form bringen

$$(2) \qquad \begin{aligned} & (\alpha\varkappa + \beta)^2 \cdot [\alpha^2(cg - e^2) + 2\alpha\beta(de - bg) + 2\alpha\gamma(be - cd) \\ & \qquad + \beta^2(ag - d^2) + 2\beta\gamma(bd - ae) + \gamma^2(ac - b^2)], \end{aligned}$$

und da der erste Factor nicht verschwinden kann, ohne die Existenz des Systems zu zerstören, so liefert das Verschwinden der eckigen Klammer in (2) die charakteristische Bedingung dafür, dass das betrachtete System eine Doppelwurzel besitzt.

Wir können aber weiter, gestützt auf die in § 399 abgeleiteten Resultate, die Frage noch von einer anderen Seite her betrachten. Wir haben dort gesehen, dass das Verschwinden der Functionaldeterminante

$$(3) \qquad J(z_1, z_2, \cdots z_m) = \frac{\partial(f_1, f_2, \cdots f_m)}{\partial(z_1, z_2, \cdots z_m)} = \left| \frac{\partial f_\varkappa}{\partial z_\lambda} \right|$$

für eine Wurzel $(\zeta_1, \zeta_2, \cdots \zeta_m)$ des Systems (1) charakteristisch dafür ist, dass diese Wurzel eine Multiplicität > 1 besitzt. Sind also $(\zeta_{1\alpha}, \zeta_{2\alpha}, \cdots \zeta_{m\alpha})$ für $\alpha = 1, 2, \cdots k$ sämmtliche Wurzeln von (1), deren

Anzahl als endlich vorausgesetzt war, so folgt: Das Verschwinden der Function

$$\prod_{\alpha} J(\zeta_{1\alpha}, \zeta_{2\alpha}, \cdots \zeta_{m\alpha}) \qquad (\alpha = 1, 2, \cdots k) \tag{4}$$

ist charakteristisch dafür, dass das System (1) mehrfache Wurzeln besitzt. Der Ausdruck (4) ist in den Wurzeln von (1) symmetrisch und also rational durch die Coefficienten von (1) darstellbar. Hieraus erkennen wir, dass eine einzige Relation die Frage entscheidet; folglich muss aus der Discriminante der Eliminationsgleichung $R(x) = 0$ der Ausdruck (4) so als Factor heraustreten, dass der zurückbleibende, von den x abhängige Factor nicht gleich Null gesetzt werden kann, so lange das Gleichungssystem (1) bestehen bleibt.

Bei der Berechnung von (4) ist zur Umsetzung der Function in einen Ausdruck, welcher nur die Coefficienten der f_α enthält, wieder die Kenntniss der Coefficienten von $R(x)$ nothwendig.

Im behandelten Beispiele wird

$$\begin{aligned}
(a\beta^2 - 2b\alpha\beta + c\alpha^2)(\zeta_{11} + \zeta_{12}) &= 2(b\beta\gamma - c\alpha\gamma - d\beta^2 + e\alpha\beta),\\
(a\beta^2 - 2b\alpha\beta + c\alpha^2)(\zeta_{21} + \zeta_{12}) &= 2(-a\beta\gamma + b\alpha\gamma + d\alpha\beta - e\alpha^2),\\
(a\beta^2 - 2b\alpha\beta + c\alpha^2)\cdot\zeta_{11}\zeta_{12} &= c\gamma^2 - 2e\beta\gamma + g\beta^2,\\
(a\beta^2 - 2b\alpha\beta + c\alpha^2)\cdot\zeta_{21}\zeta_{22} &= a\gamma^2 - 2d\alpha\gamma + g\alpha^2,\\
(a\beta^2 - 2b\alpha\beta + c\alpha^2)(\zeta_{11}\zeta_{22} + \zeta_{21}\zeta_{12}) &= 2(-b\gamma^2 + d\beta\gamma + e\alpha\gamma - g\alpha\beta).
\end{aligned}$$

Ferner ist

$$\frac{1}{2} J(z_1, z_2) = (a\beta - b\alpha)z_1 + (b\beta - c\alpha)z_2 + (d\beta - e\alpha),$$

und

$$\begin{aligned}
&\frac{1}{4} J(\zeta_{11}, \zeta_{21}) J(\zeta_{12}, \zeta_{22})\\
&= (a\beta - b\alpha)^2\zeta_{11}\zeta_{12} + (a\beta - b\alpha)(b\beta - c\alpha)(\zeta_{11}\zeta_{22} + \zeta_{21}\zeta_{12})\\
&+ (b\beta - c\alpha)^2\zeta_{21}\zeta_{22} + (a\beta - b\alpha)(d\beta - e\alpha)(\zeta_{11} + \zeta_{12})\\
&+ (b\beta - c\alpha)(d\beta - e\alpha)(\zeta_{21} + \zeta_{22}) + (d\beta - e\alpha)^2.
\end{aligned}$$

Trägt man die Werthe für die symmetrischen Functionen ein, dann entsteht wieder die eckige Klammer in (2).

Wir wollen nachweisen, dass der Ausdruck (4) von mehrfachen Factoren frei ist, so lange die Functionen (1) allgemein bleiben. Dazu reicht es aus, diese Eigenschaft an einem passend gewählten Beispiele zu zeigen, bei welchem natürlich keine Reductionen der Dimension eintreten dürfen. Ein solches Beispiel erhält man, sobald jedes f_α in n_α lineare Factoren zerlegbar angenommen wird. Wir setzen $m = 2$, weil schon hierbei die Schlussfolgerungen deutlich heraustreten,

$$f_1 = \prod (a_{\alpha 1} z_1 + a_{\alpha 2} z_2 + a_{\alpha 0}) = \prod u_\alpha \qquad (\alpha = 1, 2, \cdots n_1),$$
$$f_2 = \prod (b_{\alpha 1} z_1 + b_{\alpha 2} z_2 + b_{\alpha 0}) = \prod v_\alpha \qquad (\alpha = 1, 2, \cdots n_2).$$

Wir bezeichnen die Wurzel von $u_\alpha = 0$, $v_\beta = 0$ mit $(\zeta_1^{\alpha,\beta}, \zeta_2^{\alpha,\beta})$, dann ist

$$(5) \quad \begin{aligned} u_\gamma(\zeta_1^{\alpha,\beta}, \zeta_2^{\alpha,\beta}) &= \begin{vmatrix} a_{\gamma 1} & a_{\gamma 2} & a_{\gamma 0} \\ a_{\alpha 1} & a_{\alpha 2} & a_{\alpha 0} \\ b_{\beta 1} & b_{\beta 2} & b_{\beta 0} \end{vmatrix} : \begin{vmatrix} a_{\alpha 1} & a_{\alpha 2} \\ b_{\beta 1} & b_{\beta 2} \end{vmatrix}, \\ v_\gamma(\zeta_1^{\alpha,\beta}, \zeta_2^{\alpha,\beta}) &= \begin{vmatrix} b_{\gamma 1} & b_{\gamma 2} & b_{\gamma 0} \\ a_{\alpha 1} & a_{\alpha 2} & a_{\alpha 0} \\ b_{\beta 1} & b_{\beta 2} & b_{\beta 0} \end{vmatrix} : \begin{vmatrix} a_{\alpha 1} & a_{\alpha 2} \\ b_{\beta 1} & b_{\beta 2} \end{vmatrix}. \end{aligned}$$

Der Ausdruck (4) geht, wie man leicht sieht, in

$$(6) \quad \prod \begin{vmatrix} a_{p1} & a_{p2} \\ b_{q1} & b_{q2} \end{vmatrix} u_\alpha(\zeta_1^{p,q}, \zeta_2^{p,q})\, v_\beta(\zeta_1^{p,q}, \zeta_2^{p,q})$$
$$(p = 1, 2, \cdots n_1;\ q = 1, 2, \cdots n_2;$$
$$\alpha = 1, 2, \cdots p-1, p+1, \cdots n_1;\ \beta = 1, 2, \cdots q-1, q+1, \cdots n_2)$$

über, und aus (5) ist ersichtlich, dass keinerlei vielfache Factoren in (6) auftreten, wenn die a, b als unbestimmte Grössen genommen werden.

§ 453. In dem Falle, dass $k = n_1 \cdot n_2, \cdots n_m$ ist, wenn also (1) keine unendlichen Wurzeln hat, lässt (4) noch eine weitere merkwürdige Umformung zu, welche einen Ausdruck liefert ähnlich dem, der die Discriminante als Quadrat einer Determinante darstellt*).

Wir untersuchen die bereits in § 352 betrachtete Determinante

$$\Delta_0 = \left| 1, \zeta_{1\alpha}, \zeta_{2\alpha}, \cdots \zeta_{1\alpha}^2, \zeta_{1\alpha}\zeta_{2\alpha}, \cdots \zeta_{1\alpha}^{n_1-1}, \cdots \zeta_{2\alpha}^{n_2-1}, \cdots \zeta_{m\alpha}^{n_m-1} \right|,$$

in welcher die einzelnen Zeilen durch die Coordinaten der verschiedenen Wurzeln von (1), also durch den Index α sich unterscheiden, und in deren Elementen alle Potenzproducte auftreten, welche in ζ_1 nicht die n_1^{te}, in ζ_2 nicht die $n_2^{\text{te}}, \cdots$ Potenz erreichen. Die Determinante ist also vom Grade $(n_1 \cdot n_2, \cdots n_m)$. Wir wollen ihre Dimension in den ζ aufsuchen. Wir nehmen an, es sei schon für $(m-1)$ Grössen ζ bewiesen, dass die Dimension der Determinante Δ_0 dabei

$$\frac{1}{2}(n_1 \cdot n_2 \cdots n_{m-1}) \sum (n_\alpha - 1) \qquad (\alpha = 1, 2, \cdots m)$$

sei. Tritt dann ζ_m dazu, dann kommt für die Subdeterminanten aus den mit $\zeta_{m1}^{\varrho}, \zeta_{m2}^{\varrho}, \cdots$ multiplicirten Gliedern als Dimension

*) **Laurent**: Traité d'Analyse. Paris (1885), I. p. 305—306.

$$\frac{1}{2}(n_1 n_2 \cdots n_{m-1}) \sum_1^{m-1} (n_\alpha - 1) + \varrho \cdot (n_1 n_2 \cdots n_{m-1})$$

heraus. Man findet als Dimensionszahl, indem man alle diese für $\varrho = 0, 1, \cdots, n_m - 1$ gebildeten Ausdrücke summirt,

$$(7) \quad \begin{aligned} &\frac{1}{2}(n_1 n_2 \cdots n_{m-1}) n_m \sum_1^{m-1} (n_\alpha - 1) + \frac{n_m(n_m-1)}{2}(n_1 n_2 \cdots n_{m-1}) \\ &= \frac{1}{2}(n_1 n_2, \cdots n_m) \sum_1^m (n_\alpha - 1); \end{aligned}$$

es tritt also wieder die oben angenommene Form heraus, die für $m = 1$ offenbar richtig ist. Folglich gilt sie allgemein.

Nun verschwindet Δ_0, sobald (1) eine mehrfache Wurzel hat, und ferner ist Δ_0^2 symmetrisch in den Wurzeln. Das Verschwinden des Ausdrucks (4) war aber charakteristisch dafür, dass mehrfache Wurzeln vorkommen; daher ist Δ_0^2 durch alle irreductiblen Factoren von (4) und also, da (4) keine mehrfachen Factoren besitzt, durch (4) selbst theilbar, und der Quotient ist wieder eine symmetrische Function der ζ. Die Dimension von (4) beträgt $k \cdot \Sigma(n_\alpha - 1)$, also genau so viel wie diejenige von Δ_0^2. Folglich stimmen (4) und Δ_0^2 bis auf einen von ζ unabhängigen Factor überein, und man hat

$$(8) \quad \prod_\alpha J(\zeta_{1\alpha}, \cdots \zeta_{m\alpha}) = c \cdot \Delta_0^2 \qquad (\alpha = 1, 2, \cdots, n_1 n_2 \cdots n_m).$$

Nach den bisherigen Betrachtungen dürfen wir diesen Ausdruck als die Discriminante des Gleichungssystems (1) bezeichnen.

§ 454. Neben diese Verallgemeinerung des Discriminantenbegriffes durch den Uebergang von einer Gleichung mit einer Unbekannten zu einem Systeme von m Gleichungen mit m Unbekannten tritt noch eine andere, welche wir jetzt zu besprechen haben.

Wir hatten der Discriminante von

$$f(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n$$

die Form gegeben

$$D = \frac{1}{a_0} \begin{vmatrix} a_0 & a_1 & a_2 & \cdots \\ 0 & a_0 & a_1 & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ n a_0 & (n-1)a_1 & (n-2)a_2 & \cdots \\ 0 & n a_0 & (n-1)a_1 & \cdots \\ \cdot & \cdot & \cdot & \cdots \end{vmatrix} \begin{matrix} (n-1) \text{ Zeilen,} \\ \\ \\ n \text{ Zeilen;} \end{matrix}$$

diesen Ausdruck gestalten wir folgendermassen um (§ 160, Bd. I)

$$D = \frac{1}{a_0 n^{n-1}} \begin{vmatrix} na_0 & na_1 & na_2 & \cdots \\ 0 & na_0 & na_1 & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ na_0 & (n-1)a_1 & (n-2)a_2 & \cdots \\ 0 & na_0 & (n-1)a_1 & \cdots \\ \cdot & \cdot & \cdot & \cdots \end{vmatrix}$$

$$= \frac{(-1)^{n-1}}{n^{n-2}} \begin{vmatrix} a_1 & 2a_2 & 3a_3 & \cdots \\ 0 & a_1 & 2a_2 & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ na_0 & (n-1)a_1 & (n-2)a_2 & \cdots \\ 0 & na_0 & (n-1)a_1 & \cdots \\ \cdot & \cdot & \cdot & \cdots \end{vmatrix}.$$

Es wird daher, wenn wir

$$f_1 = na_0 z^{n-1} + (n-1)a_1 z^{n-2} + (n-2)a_2 z^{n-3} + \cdots + 2a_{n-2}z + a_{n-1},$$
$$f_2 = a_1 z^{n-1} + 2a_2 z^{n-2} + 3a_3 z^{n-3} + \cdots + (n-1)a_{n-1}z + na_n$$

setzen,

$$(-1)^{n-1} n^{n-2} D = R_{f_1, f_2}$$

werden. Diese Umgestaltung lässt eine symmetrische Behandlung zu, wenn wir f durch Einführung einer neuen Variablen zu einer homogenen Form machen. Dabei folgt dann, wenn wir im Schlussresultate $y = 1$ setzen,

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_{n-1} xy^{n-1} + a_n y^n;$$
$$\frac{\partial f}{\partial x} = f_1 = na_0 x^{n-1} + (n-1)a_1 x^{n-2} y + \cdots;$$
$$\frac{\partial f}{\partial y} = f_2 = a_1 x^{n-1} + 2a_2 x^{n-2} y + \cdots;$$
$$n^{n-2} D = R_{f_2, f_1}.$$

Da in den folgenden Paragraphen dieser Vorlesung hauptsächlich von einer einzigen Function $\varphi(z_1, z_2, \cdots)$ die Rede sein wird, so wollen wir der bequemeren Schreibweise halber

$$\frac{\partial \varphi}{\partial z_1} = \varphi_1, \ \frac{\partial \varphi}{\partial z_2} = \varphi_2, \cdots; \ \frac{\partial^2 \varphi}{\partial z_1^2} = \varphi_{11}, \ \frac{\partial^2 \varphi}{\partial z_1 \partial z_2} = \varphi_{12}, \cdots$$

bezeichnen. Ferner wollen wir annehmen, φ sei homogen gemacht, aber in allen Resultaten werde die homogen machende Variable z_m gleich 1 gesetzt.

§ 455. Unsere Verallgemeinerung soll nun folgende sein: Ist eine homogene Function $\varphi(z_1, z_2, \cdots z_m)$ gegeben, so soll die Resultante R der m Ableitungen $\varphi_1, \varphi_2, \cdots \varphi_m$ als Discriminante D bezeichnet werden. Hieraus folgt, dass wenn die Discriminante D von φ verschwindet, es von $(0, 0, \cdots 0)$ verschiedene Werth-

systeme $(\zeta_1, \zeta_2, \cdots \zeta_m)$ giebt, für welche $\varphi_1 = 0$, $\varphi_2 = 0, \cdots$ und also auch

$$\varphi = \frac{1}{m}[\zeta_1\varphi_1(\zeta_1, \cdots \zeta_m) + \zeta_2\varphi_2(\zeta_1, \cdots \zeta_m) + \cdots + \zeta_m\varphi_m(\zeta_1, \cdots \zeta_m)]$$

gleich Null wird.

Die geometrische Bedeutung dieser Discriminante D erkennt man durch die folgende Betrachtung. Wir nennen jedes System $(\zeta_1, \zeta_2, \cdots \zeta_m)$, welches $\varphi(z_1, z_2, \cdots z_m) = 0$ macht, einen Punkt des Gebildes $\varphi = 0$. Von einem solchen Punkte des Gebildes $\varphi = 0$ lassen wir eine Gerade

$$(8) \qquad x_1 = \zeta_1 + \varrho y_1, \quad x_2 = \zeta_2 + \varrho y_2, \cdots x_m = \zeta_m + \varrho y_m$$

ausgehen, welche den Punkt $(\zeta_1, \zeta_2, \cdots \zeta_m)$ mit dem Punkte $(y_1, y_2, \cdots y_m)$ verbindet. In (8) laufe ϱ durch alle reellen Werthe von $-\infty$ bis $+\infty$, und der Inbegriff der so erhaltenen $(x_1, x_2, \cdots x_m)$ stellt eben die Gerade dar. Wir fragen nach den Schnittpunkten unserer Geraden mit φ. Diese werden durch die Wurzeln ϱ von $\varphi(x_1, x_2, \cdots x_m) = 0$ geliefert, und da $(\zeta_1, \zeta_2, \cdots \zeta_m)$ dem Gebilde angehört, so ist

$$\varphi(x_1, x_2, \cdots x_m) = \varrho[y_1\varphi_1(\zeta_1, \cdots \zeta_m) + y_2\varphi_2(\zeta_1, \cdots \zeta_m) + \cdots]$$
$$+ \frac{1}{2!}\varrho^2[y_1^2\varphi_{11}(\zeta_1, \cdots \zeta_m) + 2y_1y_2\varphi_{12}(\zeta_1, \cdots \zeta_m) + \cdots] + \cdots$$

gleich Null zu setzen. Die Anzahl der Wurzeln ϱ ist also gleich der Dimension von φ. Eine der Wurzeln ist $\varrho = 0$. Wählt man nun $y_1, y_2, \cdots y_m$ auf dem Gebilde

$$(9) \quad y_1\varphi_1(\zeta_1, \cdots \zeta_m) + y_2\varphi_2(\zeta_1, \cdots \zeta_m) + \cdots + y_m\varphi_m(\zeta_1, \cdots \zeta_m) = 0,$$

so werden zwei der Wurzeln ϱ gleich 0 werden. Bezeichnen wir das Gebilde (9) als Tangentialebene von $\varphi(z_1, \cdots z_m) = 0$ im Punkte $(\zeta_1, \cdots \zeta_m)$, so ist es klar, dass jede Gerade (8), welche $(\zeta_1, \cdots \zeta_m)$ und einen Punkt der Tangentialebene verbindet, mit $\varphi = 0$ in $(\zeta_1, \cdots \zeta_m) = 0$ eine Doppelwurzel $\varrho = 0$ besitzt und umgekehrt. Es ist ferner klar, dass jede solche Gerade ganz der Tangentialebene angehört. Die Gleichung (9) bestimmt im Allgemeinen die Tangentialebene eindeutig. Nur dann wird diese Bestimmung hinfällig, wenn alle Coefficienten $\varphi_1, \varphi_2, \cdots$ in (9) einzeln verschwinden. In diesem Falle existirt keine durch $(\zeta_1, \cdots \zeta_m)$ gehende Tangentialebene, sondern jede durch diesen Punkt des Gebildes gehende Gerade hat eine Doppelwurzel $\varrho = 0$ mit demselben. Diese Punkte sollen singuläre Punkte von $\varphi(z_1, \cdots z_m) = 0$ heissen. Solche singulären Punkte bestehen stets dann und nur dann, wenn die Discriminante D von φ verschwindet; sie werden durch die gemeinsamen Wurzeln von

$$\varphi_1(z_1, \cdots z_m) = 0, \quad \varphi_2(z_1, \cdots z_m) = 0, \cdots \quad \varphi_m(z_1, \cdots z_m) = 0$$

geliefert.

Ist $(\zeta_1, \cdots \zeta_m)$ ein singulärer Punkt, und wählt man $(y_1, y_2, \cdots y_m)$ auf dem Gebilde

(10) $$y_1^2\varphi_{11}(\zeta_1, \cdots \zeta_m) + 2y_1y_2\varphi_{12}(\zeta_1, \cdots \zeta_m) + \cdots = 0,$$

so erkennt man zuerst leicht aus den Sätzen über homogene Functionen, dass die gesammte Gerade (8) dem Gebilde (10) angehört, und ferner, dass jede von $(\zeta_1, \cdots \zeta_m)$ ausgehende, auf (10) liegende Gerade mit $f = 0$ in $(\zeta_1, \cdots \zeta_m)$ eine dreifache Wurzel $\varrho = 0$ hat. Das Gebilde (10) heisst der **Tangentialkegel** von $f = 0$ für den singulären Punkt $(\zeta_1, \cdots \zeta_m)$. Natürlich kann (10) auch in zwei getrennte oder zusammenfallende lineare Ausdrücke zerfallen.

Wir können dieselben Betrachtungen auch gänzlich analytisch wenden. Es sei $(\zeta_1, \cdots \zeta_m)$ ein Punkt des Gebildes $\varphi = 0$. Es soll versucht werden, ein lineares Gebilde mit festen Coefficienten p

(11) $$(y_1 - \zeta_1)p_1 + (y_2 - \zeta_2)p_2 + \cdots + (y_m - \zeta_m)p_m = 0$$

derart zu bestimmen, dass $\varphi(y_1, \cdots y_m) = 0$ mit (11) und den $(m-2)$ folgenden linearen Gleichungen

(12) $$(y_1 - \zeta_1)q_{\alpha 1} + (y_2 - \zeta_2)q_{\alpha 2} + \cdots + (y_m - \zeta_m)q_{\alpha m} = 0$$
$$(\alpha = 1, 2, \cdots m-2)$$

bei willkürlichen q stets in $(y_1, y_2, \cdots y_m) = (\zeta_1, \zeta_2, \cdots \zeta_m)$ eine mehrfache Wurzel besitze. Nach dem Satze über die Functionaldeterminante aus § 399 folgt, dass

$$\begin{vmatrix} \varphi_1(\zeta_1, \cdots \zeta_m), & \varphi_2(\zeta_1, \cdots \zeta_m), & \cdots & \varphi_m(\zeta_1, \cdots \zeta_m) \\ p_1 & , \quad p_2 & , \cdots & p_m \\ q_{11} & , \quad q_{12} & , \cdots & q_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ q_{m-2,1} & , \quad q_{m-2,2} & , \cdots & q_{m-2,m} \end{vmatrix}$$

für jede Wahl der q gleich Null sein muss. Wählt man $q_{11}, q_{12}; q_{21}, q_{22}; \cdots$ gleich Null, die übrigen q beliebig, so folgt $p_1 : p_2 = \varphi_1 : \varphi_2$, u. s. f. Man erhält also für (11) wieder die Form (9). Man erkennt übrigens sofort, dass wir die linearen Gleichungen (12) durch völlig willkürliche höhere Gleichungen hätten ersetzen können.

Auch hier zeigt es sich, dass $p_1, p_2, \cdots p_m$ ganz beliebig angenommen werden können, sobald $\varphi_1(\zeta_1, \cdots) = 0, \cdots \varphi_m(\zeta_1, \cdots) = 0$ ist.

§ 456. Da D die Resultante von $\varphi_1, \varphi_2, \cdots \varphi_m$ ist, so wird sie in den Coefficienten von φ_1 homogen von einer Dimension, welche gleich dem Producte der Dimensionen der übrigen Functionen φ ist, d. h. gleich $(n-1)^{m-1}$. Das Gleiche gilt für die Coefficienten von $\varphi_2, \varphi_3, \cdots$, und da diese sämmtlich zu den Coefficienten von φ gehören,

so sieht man: **Die Discriminante D von φ ist in den Coefficienten von φ homogen von der Dimension $m(n-1)^{m-1}$.**

Es ist ferner D in den Coefficienten aller $\varphi_1, \varphi_2, \cdots \varphi_m$ isobarisch, falls die Gewichte der Coefficienten der einzelnen Functionen in der früheren Weise festgesetzt werden, wobei nur daran zu erinnern ist, dass durch die Annahme der Homogeneität die gegebene Vorschrift formal modificirt werden muss. Ist nämlich für eine allgemeine Function von $z_1, z_2, \cdots z_{m-1}$ das Gewicht der einzelnen Coefficienten festgesetzt, und macht man dann die Function durch die Einführung einer neuen Variablen z_m homogen, dann erkennt man, dass jeder Coefficient ein Gewicht besitzt, welches dem im zugehörigen Potenzproducte auftretenden Exponenten von z_m gleich ist. Es haben also z. B. die Glieder, die z_m nicht enthalten, Coefficienten des Gewichtes 0; die Glieder, welche mit z_m^1 multiplicirt sind, Coefficienten des Gewichtes 1, u. s. f.

Ist auf diese Art das Gewicht der Coefficienten von φ festgelegt, dann erkennt man, dass durch dieselbe Regel auch die Gewichte der Coefficienten von $\varphi_1, \varphi_2, \cdots \varphi_{m-1}$ bestimmt werden. Bei φ_m dagegen wird jeder Coefficient ein um 1 erhöhtes Gewicht gegenüber dem der angegebenen Regel gemäss abgeleiteten haben; denn in den ersten Fällen bleiben ja beim Uebergange von φ auf die Ableitung die Potenzen von z_m ungeändert, im letzten Falle werden sie um eine Einheit vermindert.

Wären alle Gewichte der Coefficienten nach der angegebenen Regel bestimmt, so wäre D isobarisch vom Gewichte $(n-1)^m$. Hier tritt für φ_m bei jedem Coefficienten eine Erhöhung um 1 ein, und da die Coefficienten homogen von der Dimension $(n-1)^{m-1}$ in die Discriminante D eintreten, so ist **das Gewicht von D gleich**

$$(n-1)^m + (n-1)^{m-1} = n(n-1)^{m-1}.$$

§ 457. Wir wollen jetzt φ durch eine homogene lineare Substitution

$$z_\varkappa = q_{\varkappa 1} y_1 + q_{\varkappa 2} y_2 + \cdots + q_{\varkappa m} y_m \qquad (\varkappa = 1, 2, \cdots m)$$

transformiren, deren Determinante $\Delta = |q_{\alpha\beta}|$ von Null verschieden ist. Man hat dann, wenn

$$\varphi(z_1, z_2, \cdots z_m) = \psi(y_1, y_2, \cdots y_m)$$

gesetzt wird,

$$\psi_k = q_{1k}\varphi_1 + q_{2k}\varphi_2 + \cdots + q_{mk}\varphi_m.$$

Demnach ist nach dem zweiten Satze aus § 424 die Resultante der $\psi_1, \psi_2, \cdots \psi_m$ nach $y_1, y_2, \cdots y_m$ gleich der Resultante von $\varphi_1, \varphi_2, \cdots \varphi_m$ nach denselben Variablen multiplicirt mit der $(n-1)^{m-1}$-ten Potenz von Δ. Ferner ist nach dem ersten Satze von § 424 die Resultante der φ_α nach den y gleich der Resultante der φ nach den z multiplicirt

mit $(n-1)^m$-ten Potenz von Δ. Folglich ist die Discriminante der Function

$$\varphi(q_{11}y_1 + \cdots + q_{1m}y_m,\ q_{21}y_1 + \cdots + q_{2m}y_m, \cdots)$$

gleich der Discriminante von $\varphi(z_1, z_2, \cdots)$ multiplicirt mit

$$\Delta^{(n-1)^{m-1} + (n-1)^m} = \Delta^{n(n-1)^{m-1}}.$$

§ 458. Ist φ eine homogene, nicht lineare Form gewisser anderer Functionen $g_1, g_2, \cdots$, die so beschaffen sind, dass das System

$$g_1 = 0,\ g_2 = 0, \cdots$$

unendlich viele Wurzeln besitzt, was also z. B. stets dann eintritt, sobald die Anzahl der Variablen von φ grösser ist, als die Anzahl der g, dann verschwindet die Discriminante von φ identisch.

Hat man nämlich $\varphi = \Sigma q \cdot g_1^{\varkappa} g_2^{\lambda} \cdots$ bei $\varkappa + \lambda + \cdots > 1$, dann können $\varphi_1, \varphi_2, \cdots \varphi_m$ auf dieselbe Form gebracht werden, so dass die Gleichungen $\varphi_1 = 0$, $\varphi_2 = 0, \cdots \varphi_m = 0$ erfüllt sind, sobald $g_1 = 0$, $g_2 = 0, \cdots$ wird. Folglich hat das System $\varphi_1 = 0, \cdots \varphi_m = 0$ unendlich viele Wurzeln, und daher ist seine Resultante, d. h. die Discri minante von φ identisch 0.

Im Falle $m = 2$ sind die Voraussetzungen erfüllt, sobald φ einen mehrfachen Factor besitzt.

§ 459. Falls die Function φ einen nur einfachen singulären Punkt $(\zeta_1, \zeta_2, \cdots \zeta_m)$ hat, kann derselbe durch Differentiation von D gefunden werden.

Der Voraussetzung nach ist D von φ gleich Null; wir wollen die Coefficienten $a_0, a_1, \cdots$ von φ in $a_0 + \delta a_0$, $a_1 + \delta a_1, \cdots$ derart umwandeln, dass $D = 0$ bleibt. Dann gilt also die Gleichung

$$(13) \qquad \frac{\partial D}{\partial a_0}\delta a_0 + \frac{\partial D}{\partial a_1}\delta a_1 + \cdots = 0.$$

Durch die gemachte Umwandlung möge der singuläre Punkt $(\zeta_1, \cdots \zeta_m)$ in $(\zeta_1 + \delta\zeta_1, \cdots \zeta_m + \delta\zeta_m)$ übergehen. Dann ist auch für diesen die umgewandelte Function sowie jede ihrer Ableitungen gleich Null; also

$$\frac{\partial \varphi_\varkappa}{\partial a_0}\delta a_0 + \frac{\partial \varphi_\varkappa}{\partial a_1}\delta a_1 + \cdots + \frac{\partial \varphi_\varkappa}{\partial \zeta_1}\delta\zeta_1 + \frac{\partial \varphi_\varkappa}{\partial \zeta_2}\delta\zeta_2 + \cdots = 0$$
$$(\varkappa = 1, 2, \cdots m).$$

Wir multipliciren mit $\zeta_\varkappa$ und addiren die Producte. Weil

$$\frac{\partial \varphi_\varkappa}{\partial a_\lambda} = \frac{\partial^2 \varphi}{\partial \zeta_\varkappa \partial a_\lambda} = \frac{\partial}{\partial \zeta_\varkappa}\left(\frac{\partial \varphi}{\partial a_\lambda}\right)$$

ist, so wird der Coefficient von δa_λ gleich

$$\zeta_1 \frac{\partial}{\partial \zeta_1}\left(\frac{\partial \varphi}{\partial a_\lambda}\right) + \zeta_2 \frac{\partial}{\partial \zeta_2}\left(\frac{\partial \varphi}{\partial a_\lambda}\right) + \cdots = (n-1)\frac{\partial \varphi}{\partial a_\lambda}$$

nach dem Euler'schen Satze; und der Coefficient von $\delta \zeta_\lambda$ wird gleich

$$\zeta_1 \frac{\partial \varphi_1}{\partial \zeta_\lambda} + \zeta_2 \frac{\partial \varphi_2}{\partial \zeta_\lambda} + \cdots = \zeta_1 \frac{\partial \varphi_\lambda}{\partial \zeta_1} + \zeta_2 \frac{\partial \varphi_\lambda}{\partial \zeta_2} + \cdots = (n-1)\frac{\partial \varphi}{\partial \zeta_\lambda} = 0.$$

Man erhält also als Summe

$$\frac{\partial \varphi}{\partial a_0}\delta a_0 + \frac{\partial \varphi}{\partial a_1}\delta a_1 + \cdots = 0. \tag{14}$$

Durch die Bedingung (13) ist von den Incrementen δa_0, $\delta a_1, \cdots$ nur eins durch die anderen bestimmt, etwa δa_0 durch δa_1, $\delta a_2, \cdots$, welche willkürlich bleiben; eliminirt man nun δa_0 aus (14) und (13), so kann die resultirende Gleichung nur dann erfüllt sein, wenn die Coefficienten von δa_1, $\delta a_2, \cdots$ einzeln verschwinden, d. h. es folgt

$$\frac{\partial D}{\partial a_0} : \frac{\partial D}{\partial a_1} : \frac{\partial D}{\partial a_2} : \cdots = \frac{\partial \varphi}{\partial a_0} : \frac{\partial \varphi}{\partial a_1} : \frac{\partial \varphi}{\partial a_2} : \cdots. \tag{15}$$

Bedenkt man endlich, dass φ linear und homogen in den $a_0, a_1, \cdots$ ist, so folgt, dass jedes Glied der rechten Seite in (15) ein Potenzproduct der $\zeta_1, \zeta_2, \cdots \zeta_m$ wird. Passende Wahl der Exponenten führt also durch (15) zur Bestimmung von $\zeta_1 : \zeta_2 : \cdots : \zeta_m$ selbst. (Vgl. § 163, Bd. I.) — Bei mehrfachen Wurzeln versagt dieser Schluss.

§ 460. Wir haben im § 442 gefunden, dass wenn $f=0$, $g=0$, $h=0, \cdots$ eine Reihe von m homogenen Gleichungen der m Unbekannten $z_1, z_2, \cdots z_m$ darstellt, dann die Functionaldeterminante J dieser Gleichungen für jede Wurzel $(\zeta_1, \zeta_2, \cdots \zeta_m)$ von $f=0$, $g=0$, $h=0, \cdots$ verschwindet. Wir wollen jetzt alle diese Gleichungen von derselben Dimension n annehmen. Dann folgt aus

$$\begin{aligned} z_1 f_1 + z_2 f_2 + z_3 f_3 + \cdots + z_m f_m &= nf, \\ z_1 g_1 + z_2 g_2 + z_3 g_3 + \cdots + z_m g_m &= ng, \\ \cdots\cdots\cdots & \end{aligned}$$

durch Auflösung nach den z die Relation

$$z_1 \begin{vmatrix} f_1, & f_2, & \cdots \\ g_1, & g_2, & \cdots \\ \cdot & \cdot & \cdots \end{vmatrix} = n \begin{vmatrix} f, & f_2, & \cdots \\ g, & g_2, & \cdots \\ \cdot & \cdot & \cdots \end{vmatrix},$$

wobei der Coefficient von z_1 gleich J ist. Differentiirt man nach z_2, so folgt

$$n[f\cdot F_2 + g\cdot G_2 + h\cdot H_2 + \cdots] = z_1 J_2;$$

denn die Differentiation nach den Elementen der ersten Spalte der Determinante rechts ergiebt eine verschwindende Determinante. Ebenso ist

$$n[f\cdot F_3 + g\cdot G_3 + h\cdot H_3 + \cdots] = z_1 J_3, \quad \text{u. s. w.}$$

Für $(\zeta_1, \zeta_2, \cdots \zeta_m)$ verschwindet also ausser J auch noch $J_2, J_3, \cdots J_m$ und also auch J_1, d. h. jede der ersten Ableitungen. Also ist die Discriminante der Functionaldeterminante $J(z_1, \cdots)$ Null, wenn das System $f = 0$, $g = 0, \cdots$ der m homogenen Gleichungen eine Wurzel besitzt. Im Falle $m = 2$ hat deshalb J jeden gemeinsamen Factor $(\varkappa_0 z_1 + \lambda_0 z_2)$ von f und g als Doppelfactor.

Fünfundvierzigste Vorlesung.

Jacobi's Erweiterung eines Euler'schen Satzes.

§ 461. Im § 38, Bd. I haben wir merkwürdige, von Euler stammende Formeln abgeleitet. Jacobi hat ein Analogon zu denselben für zwei Functionen mit zwei Variablen gefunden*). Sein Beweis kann ohne Schwierigkeit auf m Functionen f_α von m Variablen $z_1, z_2, \cdots z_m$ übertragen werden.

Wir benutzen die Bézout'schen Eliminationsformeln (§ 412) und setzen, nachdem die f vorläufig präparirt sind,

$$
(1) \qquad \begin{aligned}
\varphi_{11} f_1 + \varphi_{12} f_2 + \cdots + \varphi_{1m} f_m &= G_1(z_1), \\
\varphi_{21} f_1 + \varphi_{22} f_2 + \cdots + \varphi_{2m} f_m &= G_2(z_2), \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\
\varphi_{m1} f_1 + \varphi_{m2} f_2 + \cdots + \varphi_{mm} f_m &= G_m(z_m).
\end{aligned} \qquad [G_\alpha] = k,
$$

Die Wurzeln von $G_\alpha(z_\alpha) = 0$ seien $\zeta_{\alpha 1}, \zeta_{\alpha 2}, \cdots \zeta_{\alpha\beta}, \cdots$, und zwar mögen $(\zeta_{1\varkappa}, \zeta_{2\varkappa}, \cdots \zeta_{m\varkappa})$ die Wurzeln der $f_\alpha = 0$ werden. Die Determinante der $\varphi_{\varkappa\lambda}$ bezeichnen wir mit Φ. Geben wir nun den $z_1, z_2, \cdots z_m$ irgend welche Werthe $\zeta_{1\alpha}, \zeta_{2\beta}, \cdots \zeta_{m\delta}$, welche die $G_\alpha = 0$ machen, aber nicht das System der $f_1, f_2, \cdots f_m$, dann folgt aus (1), dass Φ verschwinden muss. Es gilt also der Satz: Die Determinante

$$
(2) \qquad \Phi(z_1, z_2, \cdots z_m) = |\varphi_{\varkappa\lambda}| \qquad (\varkappa, \lambda = 1, 2, \cdots m)
$$

verschwindet für jedes System $\zeta_{1\alpha}, \zeta_{2\beta}, \cdots \zeta_{m\delta}$, welches die $G_\alpha(z_\alpha) = 0$ befriedigt, aber nicht die $f_\alpha(z_1, \cdots z_m) = 0$.

Zu einem zweiten Theoreme kommen wir auf folgende Art: Differentiirt man eine der Gleichungen (1) nach einer der Variablen z_β, so entsteht, wenn $\delta_{\alpha\beta}$ nach Kronecker 1 oder Null bedeutet, jenachdem wir $\alpha = \beta$ oder $\alpha \neq \beta$ haben,

---

*) J. f. Math. 14 (1835), p. 281. — Werke III, p. 285.

$$\sum_{\varkappa=1}^{m} \varphi_{\alpha\varkappa} \frac{\partial f_\varkappa}{\partial z_\beta} + \sum_{\varkappa=1}^{m} f_\varkappa \frac{\partial \varphi_{\alpha\varkappa}}{\partial z_\beta} = \delta_{\alpha\beta} \cdot \frac{\partial}{\partial z_\beta} G_\beta(z_\beta) = \delta_{\alpha\beta} \cdot G'_\beta(z_\beta).$$

Trägt man in diese Gleichung irgend ein Wurzelsystem $(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})$ ein, für welches alle $f_\varkappa$ verschwinden, so erhält man

$$\sum_{\varkappa=1}^{m} \varphi_{\alpha\varkappa}(\zeta_{1\gamma}, \cdots) \left| \frac{\partial f_\varkappa}{\partial z_\beta} \right|_{z=\zeta} = \delta_{\alpha\beta} G'_\beta(\zeta_{\beta\gamma}).$$

Wegen des Multiplicationssatzes für Determinanten folgt daraus

$$\Phi(\zeta_{1\gamma}, \cdots \zeta_{m\gamma}) \cdot J(\zeta_{1\gamma}, \cdots \zeta_{m\gamma}) = \prod_{\varkappa=1}^{m} G'_\varkappa(\zeta_{\varkappa\gamma}). \tag{3}$$

Wir wollen annehmen, dass die $f_\alpha = 0$ $(\alpha = 1, 2, \cdots m)$ keine mehrfachen Wurzeln besitzen. Durch unsere Vorbereitung der Functionen können wir es dann bewirken, dass auch keine der Gleichungen $G_\beta(z) = 0$ mehrfache Wurzeln hat; also bleiben die beiden Seiten von (3) für jedes γ von Null verschieden. Insbesondere ist

$$\Phi(\zeta_{1\gamma}, \cdots \zeta_{m\gamma}) \neq 0.$$

§ 462. Wir haben nun das in § 106, Bd. I bewiesene Cauchy'sche Theorem anzuwenden. Da es aber in etwas abweichender Form gebraucht wird, so mag hier noch ein directer Nachweis für diese Platz finden. Es sei eine Gleichung $f(z) = 0$ mit den untereinander verschiedenen Wurzeln $z_1, z_2, \cdots z_n$ gegeben; $M(z)$ sei irgend eine ganze Function von z. Dann lässt sich, wenn E die grösste ganze Function bedeutet, die in $M : f$ enthalten ist,

$$\begin{aligned}
\frac{M(z)}{f(z)} &= E(z) + \frac{m(z)}{f(z)} \\
&= E(z) + \sum_{\varkappa=1}^{n} \frac{m(z_\varkappa)}{f'(z_\varkappa)} \frac{1}{z - z_\varkappa} \\
&= E(z) + \sum \frac{m(z_\varkappa)}{f'(z_\varkappa)} \cdot z^{-1} + q_2 z^{-2} + \cdots \\
&= E(z) + \sum \frac{E(z_\varkappa) f(z_\varkappa) + m(z_\varkappa)}{f'(z_\varkappa)} z^{-1} + q_2 z^{-2} + \cdots \\
&= E(z) + \sum \frac{M(z_\varkappa)}{f'(z_\varkappa)} z^{-1} + q_2 z^{-2} + \cdots
\end{aligned}$$

schreiben. Es ist also die symmetrische Function

$$\sum_{\varkappa=1}^{n} \frac{M(z_\varkappa)}{f'(z_\varkappa)}$$

gleich dem Coefficienten von z^{-1} in der nach fallenden Potenzen von z geordneten Entwickelung von $M(z) : f(z)$.

Hiernach ist also die auf alle $\zeta_{1\alpha}$ $(\alpha = 1, 2, \cdots k)$ bezogene symmetrische Function

$$\sum_{(\alpha)} \frac{M(\zeta_{1\alpha}, z_2, \cdots z_m)}{G_1'(\zeta_{1\alpha}) G_2'(z_2) \cdots G_m'(z_m)} \tag{4}$$

gleich dem Coefficienten von z_1^{-1} in der Entwickelung nach z_1 von

$$\frac{M(z_1, z_2, \cdots z_m)}{G_1(z_1) G_2(z_2) \cdots G_m(z_m)}; \tag{5}$$

wenden wir denselben Satz auf (4) an, so folgt, dass die auf alle $\zeta_{1\alpha}$ und auf alle $\zeta_{2\beta}$ bezogene symmetrische Function

$$\sum_{(\alpha,\beta)} \frac{M(\zeta_{1\alpha}, \zeta_{2\beta}, z_3, \cdots z_m)}{G_1'(\zeta_{1\alpha}) G_2'(\zeta_{2\beta}) G_3'(z_3) \cdots G_m'(z_m)}$$

gleich dem Coefficienten von $(z_1 z_2)^{-1}$ in der Entwickelung von (5) nach z_1 und z_2 ist, u. s. f. und schliesslich zeigt sich, dass

$$\sum_{(\alpha,\beta,\cdots\delta)} \frac{M(\zeta_{1\alpha}, \zeta_{2\beta}, \cdots \zeta_{m\delta})}{G_1'(\zeta_{1\alpha}) G_2'(\zeta_{2\beta}) \cdots G_m'(\zeta_{m\delta})}$$

gleich dem Coefficienten von $(z_1 z_2 \cdots z_m)^{-1}$ in (5) wird.

Für M werde nun $M \cdot \Phi$ gesetzt; dann ergiebt sich unter Berücksichtigung der ersten Theoreme aus dem vorigen Paragraphen, dass

$$\sum_{\alpha} \frac{M(\zeta_{1\alpha}, \cdots \zeta_{m\alpha}) \Phi(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})}{G_1'(\zeta_{1\alpha}) \cdots G_m'(\zeta_{m\alpha})},$$

oder wegen (3), dass

$$\sum_{\alpha} \frac{M(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})}{J(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})} \tag{6}$$

gleich dem Coefficienten von $(z_1 z_2 \cdots z_m)^{-1}$ in dem nach fallenden Potenzen der z geordneten Ausdrucke

$$\frac{M(z_1, \cdots z_m) \Phi(z_1, \cdots z_m)}{G_1(z_1) G_2(z_2) \cdots G_m(z_m)} \tag{7}$$

wird.

Nun steigen die $G_1, G_2, \cdots$ bis zu dem Grade k auf, welcher dem Grade der Eliminante $R(x)$ gleichkommt. Der Nenner in (7) hat also die Dimension km. Ferner steigen die $\varphi_{\varkappa\alpha}$ im Allgemeinen bis zur Dimension $(k - n_\varkappa)$, und also steigt Φ im Allgemeinen bis zu der Dimension $(mk - \Sigma n_\varkappa)$.

Endlich bezeichnen wir mit μ die Dimension von M. Dann hat der Ausdruck (7) die Dimension $(\mu - \Sigma n_\varkappa)$. Ist nun

$$\mu - \Sigma n_\varkappa < -m$$

oder

$$\mu < \Sigma n_\varkappa - m,$$

dann kommt in der Entwickelung von (7) gar kein Glied mit $(z_1 \cdots z_m)^{-1}$ vor; folglich wird (6) gleich Null. Unsere früheren Untersuchungen über die Bézout'sche Eliminationsmethode zeigen, dass im allgemeinen Falle die angegebenen Dimensionen der $\varphi_{\alpha\beta}$ auftreten; diejenige von Φ könnte $(mk - \Sigma n_\varkappa - \varrho)$ sein, wobei ϱ eine positive Zahl bedeutet; dadurch aber würde die rechte Seite der letzten Ungleichung nur noch vergrössert werden. Wir haben daher den Jacobi'schen Satz: Bedeuten die f_α allgemeine Functionen der Dimensionen n_α, und ist M eine Function der Dimension μ, wobei $\mu < \Sigma n_\varkappa - m$ ist, dann wird

$$(8) \qquad \sum_\alpha \frac{M(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})}{J(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})} = 0.$$

Man sieht aber leicht, dass in besonderen Fällen die Bestimmung der Dimensionen für die $\varphi_{\alpha\beta}$ und für Φ hinfällig wird. Nehmen wir etwa

$$f_1 \equiv z_1^2 + z_2^2 - 9 = 0, \qquad f_2 \equiv z_1^2 + z_2^2 + 2z_1 - z_2 - 3 = 0$$

mit den beiden Wurzeln

$$(\zeta_{11}, \zeta_{21}) = (-3, 0), \qquad (\zeta_{12}, \zeta_{22}) = \left(-\frac{9}{5}, \frac{12}{5}\right),$$

dann werden die Gleichungen (1) zu

$$(2z_1 + z_2 + 5)\cdot(z_1^2 + z_2^2 - 9) - (2z_1 + z_2 + 6)\cdot(z_1^2 + z_2^2 + 2z_1 - z_2 - 3)$$
$$= -5z_1^2 - 24z_1 - 27,$$

$$(2z_1 + z_2 - 2)\cdot(z_1^2 + z_2^2 - 9) - (2z_1 + z_2 - 6)\cdot(z_1^2 + z_2^2 + 2z_1 - z_2 - 3)$$
$$= 5z_2^2 - 12z_2;$$

$$\Phi(z_1, z_2) = 10z_1 + 5z_2 + 18;$$
$$J(z_1, z_2) = -2z_1 - 4z_2.$$

Hier übertrifft die Dimension der $\varphi_{\varkappa\alpha}$ die Differenz $(k - n_\varkappa)$, und andererseits ist die Dimension von Φ geringer als die durch Gradabzählung erlangte. In Specialfällen verliert also der Jacobi'sche Satz seine Giltigkeit. In dem angeführten Beispiele hat (7) die Dimension $(\mu - 3)$; nur für $\mu = 0$ ist (8) erfüllt.

§ 463. Kronecker hat zuerst auf diesen Umstand aufmerksam gemacht*), doch habe ich in den hinterlassenen Papieren Jacobi's eine Bemerkung gefunden, aus welcher hervorgeht, dass er selbst schon für die Gültigkeit des Satzes die Bedingung als nothwendig erkannt hatte, k müsse $= n_1 \cdot n_2 \cdots n_m$ sein**).

---

*) Berl. Ber. (1863), 21. Dec.

**) Vgl. Werke III, p. 610.

Kronecker schlägt bei seiner Herleitung von (8) einen von dem obigen ganz verschiedenen Weg ein. Er geht von der in § 350 gegebenen Darstellung aus

$$(9)\qquad f_\alpha(z_1, \cdots z_m) = (z_1 - \zeta_{1\gamma})g_{\alpha 1}^{(\gamma)} + \cdots + (z_m - \zeta_{m\gamma})g_{\alpha m}^{(\gamma)}$$
$$(\alpha = 1, 2, \cdots m;\ \gamma = 1, 2, \cdots k);$$

hierin sind die $g_{\alpha\varkappa}^{(\gamma)}$ ganze Functionen von $z_1, z_2, \cdots z_m$ und von $\zeta_{1\gamma}, \zeta_{2\gamma}, \cdots \zeta_{m\gamma}$. Eine solche Darstellung ist auf unendlich viele Arten möglich; gesetzt wir hätten neben (9) auch noch

$$(9^a)\qquad f_\alpha(z_1, \cdots z_m) = (z_1 - \zeta_{1\gamma})h_{\alpha 1}^{(\gamma)} + \cdots + (z_m - \zeta_{m\gamma})h_{\alpha m}^{(\gamma)}$$
$$(\alpha = 1, 2, \cdots m;\ \gamma = 1, 2, \cdots k),$$

dann folgt, dass die Differenz der beiden rechten Seiten von (9^a) und (9) identisch, d. h. für jede Wahl der $z_1, z_2, \cdots z_m$ verschwinden muss. Es ist demnach

$$(z_1 - \zeta_{1\gamma})[h_{\alpha 1}^{(\gamma)} - g_{\alpha 1}^{(\gamma)}] + \cdots + (z_m - \zeta_{m\gamma})[h_{\alpha m}^{(\gamma)} - g_{\alpha m}^{(\gamma)}] \equiv 0.$$

Setzen wir hierin bei unbestimmtem z_1 für $z_2, \cdots z_m$ ein $\zeta_{2\gamma}, \cdots \zeta_{m\gamma}$, so folgt, dass $(h_{\alpha 1}^{(\gamma)} - g_{\alpha 1}^{(\gamma)})$ für jedes z_1 also identisch verschwinden wird. Es ist demnach

$$h_{\alpha 1}^{(\gamma)} - g_{\alpha 1}^{(\gamma)} \equiv 0 \quad (\text{modd.}\ (z_2 - \zeta_{2\gamma}),\ (z_3 - \zeta_{3\gamma}), \cdots (z_m - \zeta_{m\gamma})),$$

und in Folge dessen für $\varkappa = 1, 2, \cdots m$

$$(10)\qquad h_{\alpha\varkappa}^{(\gamma)} - g_{\alpha\varkappa}^{(\gamma)} \equiv 0 \quad (\text{modd.}\ (z_1 - \zeta_{1\gamma}), \cdots (z_m - \zeta_{m\gamma})).$$

Es ist deswegen nach dem gleichen Modulsystem auch die Determinante D_γ aus den $h_{\varkappa\lambda}^{(\gamma)}$ derjenigen aus den $g_{\varkappa\lambda}^{(\gamma)}$ congruent.

Eine solche Darstellung (9^a) können wir leicht auf folgende Weise erlangen. Es sei u_α der Complex der Glieder von der Dimension n_α aus f_α; dann wird

$$u_\alpha = \frac{1}{n_\alpha}\left(z_1 \frac{\partial u_\alpha}{\partial z_1} + \cdots + z_m \frac{\partial u_\alpha}{\partial z_m}\right),$$

$$f_\alpha = \frac{1}{n_\alpha}\left[(z_1 - \zeta_{1\gamma})\frac{\partial u_\alpha}{\partial z_1} + \cdots + (z_m - \zeta_{m\gamma})\frac{\partial u_\alpha}{\partial z_m}\right] + q_\alpha(z_1, \cdots z_m;\ \zeta_{1\gamma}, \cdots),$$

wobei q_α in den z höchstens von der Dimension $(n_\alpha - 1)$ ist und für $z_1 = \zeta_{1\gamma}, \cdots$ verschwindet. Wendet man das gleiche Verfahren auf q_α an und geht so fort, dann erkennt man, dass gesetzt werden kann

$$(11)\qquad h_{\alpha\varkappa}^{(\gamma)} = \frac{1}{n_\alpha}\frac{\partial u_\alpha}{\partial z_\varkappa} + (\text{Glieder niederer Dimension}).$$

Hieraus ergiebt sich

(12) $$D_\gamma = \left|h_{\varkappa\lambda}^{(\gamma)}\right| = \frac{1}{n_1 n_2 \cdots n_m} J_u(z_1, \cdots z_m)$$
$$+ \text{(Glieder niederer Dimensionen)},$$

wobei J_u die Functionaldeterminante der $u_1, u_2, \cdots u_m$ bedeutet.

Eine andere Form für die h können wir gewinnen, wenn wir die f_α nach Potenzen von $(z_1 - \zeta_{1\gamma}), \cdots (z_m - \zeta_{m\gamma})$ entwickeln; dann folgt, wenn wir die neuen, den $g_{\varkappa\lambda}$ entsprechenden Coefficienten mit $k_{\varkappa\lambda}$ bezeichnen,

$$k_{\varkappa\lambda}^{(\gamma)} \equiv \left|\frac{\partial f_\alpha}{\partial z_\varkappa}\right|_{z=\zeta} \quad (\text{modd. } (z_1 - \zeta_{1\gamma}), \cdots (z_m - \zeta_{m\gamma}))\,.$$

Hier wird also die Determinante der $k_{\varkappa\lambda}^{(\gamma)}$ nach dem angegebenen Modulsysteme congruent $J(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})$, wobei J wie gewöhnlich die Functionaldeterminante der f bezeichnet.

Bedenken wir weiter, dass gemäss (10) ein jedes System $k_{\varkappa\lambda}^{(\gamma)}$ (modd. $(z_1 - \zeta_{1\gamma}) \cdots$) durch die $g_{\varkappa\lambda}^{(\gamma)}$ ersetzt werden kann, so folgt, dass die Determinante D_γ für jedes System $g_{\alpha\varkappa}^{(\gamma)}$ congruent $J(\zeta_{1\gamma}, \cdots)$ ist.

Für andere Wurzeln $(\zeta_{1\delta}, \cdots \zeta_{m\delta})$ dagegen wird D_γ gleich Null; denn diese Substitution macht in (9) die linken Seiten zu Null, während nicht alle $(z_\varkappa - \zeta_{\varkappa\delta})$ verschwinden, wenn das System $f_\alpha = 0$ keine mehrfachen Wurzeln hat. Das wollen wir von jetzt ab voraussetzen.

Hiernach haben für alle Wurzeln $(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})$ $(\alpha = 1, 2, \cdots k)$ des Systems alle D_γ dieselben Werthe, wie auch die $g_{\varkappa\alpha}$ gewählt sind; nämlich für $\alpha \neq \gamma$ den Werth 0 und für $\alpha = \gamma$ den Werth $J(\zeta_{1\gamma}, \cdots)$. Folglich sind alle D_γ einander (modd. $f_1, f_2, \cdots f_m$) nach den Sätzen aus § 428 congruent. Denn die Differenz zweier D_γ verschwindet für alle Wurzeln des Systems, und diese haben nur die Multiplicität 1.

§ 464. In dem Quotienten

$$\frac{D_\gamma(z_1, z_2, \cdots z_m)}{D_\gamma(\zeta_{1\gamma}, \zeta_{2\gamma}, \cdots \zeta_{m\gamma})},$$

den wir kürzer mit $D_\gamma : \Delta_\gamma$ bezeichnen wollen, haben wir einen Ausdruck, der sich zur Erweiterung der Lagrange'schen Interpolationsformel eignet, da das Aggregat, in dem $q_1, q_2, \cdots q_k$ Constanten bedeuten,

(13) $$Q = \sum_{(\gamma)} q_\gamma \frac{D_\gamma}{\Delta_\gamma},$$

für jede Wurzel $(\zeta_{1\gamma}, \zeta_{2\gamma}, \cdots \zeta_{m\gamma})$ des Systems $f_\alpha = 0$ den Werth q_γ annimmt. Der Unterschied zwischen dieser Formel und der in § 352 gegebenen ist augenfällig; hier sind die ζ als Wurzeln eines Gleichungssystems definirt; dort waren es gegebene, bekannte Werthsysteme.

Gesetzt es gäbe eine andere Function der z, welche gleichfalls für alle $(\zeta_{1\gamma}, \cdots)$ die Werthe q_γ annimmt, dann verschwindet die Differenz dieser Function und der Function (13) für alle Wurzeln des Gleichungssystems. Da nun die Voraussetzung gemacht worden ist, dass diese sämmtlich nur einfache Wurzeln sind, so ist schon die Differenz und nicht erst die Differenz einer höheren Potenz beider Functionen congruent 0 (modd. $f_1, \cdots$). Jede Function, die für $(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})$ gleich q_γ wird $(\gamma = 1, 2, \cdots k)$, ist congruent (13) nach dem Modulsysteme $f_1, f_2, \cdots f_m$.

Wir nehmen nun eine Function $Q(z_1, z_2, \cdots z_m)$, deren Dimension geringer sein soll als die von $J(z_1, \cdots z_m)$ oder, was ja das Gleiche ist, als die von $J_u(z_1, \cdots z_m)$. Dann wählen wir für die g diejenigen Functionen, welche auf (12) führen, und haben, wenn man $Q(\zeta_{1\gamma}, \cdots) = q_\gamma$ setzt, nach (12) und (13) für Q die Darstellung

$$Q \equiv \frac{1}{n_1 \cdots n_m} J_u(z_1, \cdots z_m) \sum_{(\gamma)} \frac{q_\gamma}{\Delta_\gamma} + \text{(Glieder niederer Dimensionen)}$$

$$(\text{modd. } f_1, f_2, \cdots f_m).$$

Da nun Q von geringerer Dimension ist, als J_u, so lässt sich

$$J_u(z_1, \cdots z_m) \sum_{(\gamma)} \frac{q_\gamma}{\Delta_\gamma}$$

durch Hinzufügung eines linearen homogenen Ausdrucks von $f_1, \cdots f_m$ auf niedrigere Dimension reduciren, so dass also etwa in

$$J_u(z_1, \cdots z_m) \sum_{(\gamma)} \frac{q_\gamma}{\Delta_\gamma} - (P_1 f_1 + \cdots + P_m f_m)$$

die Glieder höchster Dimension von J_u verschwinden. Nun ist J_u homogen; behält man in den P und den f nur die Glieder höchster Dimension bei, die wir mit $u_1, u_2, \cdots$ bezeichneten, so folgt die Gleichung

$$J_u(z_1, \cdots z_m) \sum_{(\gamma)} \frac{q_\gamma}{\Delta_\gamma} = p_1 u_1 + \cdots + p_m u_m.$$

Wäre die Summe von Null verschieden, so müssten nach § 443 $u_1 = 0, u_2 = 0, \cdots u_m = 0$ gemeinsame Wurzeln haben; also wären Wurzeln von $f_1 = 0, \cdots$ unendlich, und $k < (n_1 \cdot n_2 \cdots u_m)$. Setzen wir deshalb voraus, dass $k = n_1 n_2 \cdots n_m$ ist, dann muss die Summe verschwinden. Ist die Anzahl der Wurzeln von $f_1 = 0, \cdots f_m = 0$ gleich $n_1 n_2 \cdots n_m$, und ist die Dimension von $Q(z_1, z_2, \cdots z_m)$ geringer als $(\Pi n_a - m)$, dann gilt

$$(14) \qquad \sum_{(\gamma)} \frac{Q(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})}{D_\gamma(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})} = \sum_{(\gamma)} \frac{Q(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})}{J(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})} = 0$$

und dies ist der Jacobi'sche Satz.

Es ist jetzt noch nachzuweisen, dass wenn $k < (n_1 n_2 \cdots n_m)$ wird, die Formel (14) nicht mehr allgemein gültig ist. Dazu verfahren wir folgendermassen. Da wir die Glieder höchster Dimension aus f_α mit u_α und die Functionaldeterminante der u in (12) mit J_u bezeichnet haben, so folgt jetzt die Gleichung

$$J(z_1, \cdots z_m) = J_u(z_1, \cdots z_m) + L_1(z_1, \cdots z_m),$$

in der L_1 von niederer Dimension ist als J_u, also höchstens von der Dimension $(\Sigma n_\alpha - m - 1)$. Das erkennt man sofort, wenn man die einzelnen Elemente der Determinante J nach ihren Dimensionen anordnet. Für unseren Fall $k < \Pi n_\alpha$ ist ferner J_u linear und homogen in den u_α nach § 443; also etwa

$$\begin{aligned} J_u &= q_1 u_1 + q_2 u_2 + \cdots + q_m u_m \\ &= q_1 f_1 + q_2 f_2 + \cdots + q_m f_m + L_2(z_1, \cdots z_m), \end{aligned}$$

wobei L_1 von niederer Dimension ist als $(\Sigma n_\alpha - m)$, da ja jedes f_α mit u_α in den Gliedern höchster Dimension übereinstimmt. Setzt man $L = L_1 + L_2$, so ist

$$J(z_1, \cdots z_m) \equiv L(z_1, \cdots z_m) \quad (\text{modd. } f_1, f_2, \cdots f_m),$$

und also wird für jede Wurzel $(\zeta_{1\alpha}, \cdots \zeta_{m\alpha})$

$$J(\zeta_{1\alpha}, \cdots \zeta_{m\alpha}) = L(\zeta_{1\alpha}, \cdots \zeta_{m\alpha}).$$

Es giebt demnach eine Function L von geringerer als der $(\Sigma n_\alpha - m)^{\text{ten}}$ Dimension, die für alle Wurzeln der $f_\alpha = 0$ mit der Functionaldeterminante übereinstimmt. Nehmen wir diese für Q in (14) an und bedenken, dass auch $D_\alpha(\zeta_{1\alpha}, \cdots) = J(\zeta_{1\alpha}, \cdots)$ ist (§ 463), so folgt für diese Function, dass jeder der Summanden in (14) den Werth 1 hat; also ist dafür entgegen dem Jacobi'schen Satze

$$\sum \frac{L(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})}{D_\gamma(\zeta_{1\gamma}, \cdots \zeta_{m\gamma})} = k.$$

§ 465. In noch anderer Weise zeigt Liouville*) die Richtigkeit des Satzes. Er stellt die Eliminante $R(z_1)$ von $f_1 = 0, \cdots f_m = 0$ auf verschiedene Arten her, indem er die Wurzeln $\zeta_2, \zeta_3, \cdots \zeta_m$ von je $(m-1)$ dieser Gleichungen immer in die übrigbleibende einsetzt und nach der Poisson'schen Methode das Product der Substitutionsresultate nimmt. So erhält er verschiedene Formen derselben Function R, deren

*) J. d. M. p. e. a. 6 (1841), p. 345.

Vergleichung ihm dann den Jacobi'schen Satz liefert. Derselbe tritt bei ihm in einer scheinbar grösseren Allgemeinheit auf; seine Formel lässt sich aber aus der Jacobi'schen leicht ableiten*). Setzt man nämlich statt f_1 das Product zweier Functionen $f_0 \cdot f_1$ ein, bezeichnet mit

ξ die Wurzeln, mit J_0 die Functionaldet. von $f_0, f_2, f_3, \cdots f_m$,

η " " , " J_1 " " " $f_1, f_2, f_3, \cdots f_m$

und bedenkt, dass das frühere J durch $f_0 J_1 + f_1 J_0$ ersetzt werden muss, so entsteht aus (14)

$$\sum \frac{Q(\xi_1, \cdots)}{f_1(\xi_1, \cdots) J_0(\xi_1, \cdots)} + \sum \frac{Q(\eta_1, \cdots)}{f_0(\eta_1, \cdots) J_1(\eta, \cdots)} = 0.$$

Hier ersetzt man dann Q noch durch QJ_0 und kommt zu der Liouville'schen Formel

$$\sum \frac{Q(\xi_1, \cdots)}{f_1(\xi_1, \cdots)} + \sum \frac{Q(\eta_1, \cdots) J_0(\eta_1, \cdots)}{f_0(\eta_1, \cdots) J_1(\eta_1, \cdots)} = 0,$$

welche sich sonach als einfache Folgerung aus der Jacobi'schen ausweist.

§ 466. Eine sachliche Erweiterung giebt Herr W. End: „Algebraische Untersuchungen über Flächen mit gemeinschaftlicher Curve", Math. Ann. 35 (1890), p. 82. Er weist nach (für $m = 3$), dass der Jacobi'sche Satz unter gewissen Bedingungen auch dann gilt, wenn das System der Gleichungen von höherer Stufe ist, falls nur die Summation auf diejenigen Wurzeln allein ausgedehnt wird, welche als getrennte Wurzelpunkte des Gebildes auftreten.

Sechsundvierzigste Vorlesung.

Die Kronecker'sche Charakteristiken-Theorie. Die quadratischen Formen Hermite's.

§ 467. Der Cauchy'sche Satz (§ 34, Bd. I) über die Anzahl der innerhalb einer geschlossenen einfachen Curve $C=0$ liegenden Wurzelpunkte einer Gleichung $f(z) = 0$ lässt eine bedeutende Erweiterung zu, wenn man ihn nach Einführung von $z = x + iy$ und $f(z) = u(x, y) + iv(x, y) = 0$ so auffasst, dass man das gegenseitige Durchdringen der drei Curven $C = 0$, $u = 0$, $v = 0$ studirt. Diese Betrachtungen

*) Kronecker, l. c. p. 690.

sind von Kronecker angestellt worden*). Wir wollen sie jetzt in etwas veränderter Form hier wiedergeben.

Es seien $f_0, f_1, \cdots f_m$ gegebene $(m+1)$ ganze Functionen der Variablen $z_1, z_2, \cdots z_m$ mit reellen Coefficienten; die Ableitung von f_α nach z_β bezeichnen wir mit $f_{\alpha\beta}$. Jede der Functionen f_α möge nur für endliche Werthe der Variablen verschwinden; dabei wollen wir jedem f_α ein solches Vorzeichen geben, dass für unendlich grosse z jedes f_α positiv wird. Diejenigen Stellen, in denen $\operatorname{sgn} f_\alpha = -1$ ist, nennen wir das Innere des Gebildes $f_\alpha = 0$. Es besteht aus einer oder aus mehreren geschlossenen Mannigfaltigkeiten m^{ter} Dimension.

Betrachten wir zwei solche Gebilde $f_\alpha = 0$ und $f_\beta = 0$, dann sollen diejenigen Stellen, in denen $\operatorname{sgn}(f_\alpha \cdot f_\beta) = -1$ ist, als Binnenraum für (f_α, f_β) aufgefasst werden.

Der Bequemlichkeit der Formeln wegen führen wir noch unbestimmte Elemente $f_{00}, f_{10}, \cdots f_{m0}$ ein und benutzen die Determinante

$$\varDelta = |f_{\varkappa\lambda}| \qquad (\varkappa = 0, 1, \cdots m;\ \lambda = 0, 1, \cdots m).$$

Die Ableitung $\frac{\partial \varDelta}{\partial f_{\varkappa 0}} = \varDelta_\varkappa$ ist der Functionaldeterminante $J_\varkappa$ von $f_1, \cdots f_{\varkappa-1}, f_{\varkappa+1}, \cdots f_m$ bis auf das Vorzeichen gleich; wir wollen das von $J_\varkappa$ direct gleich dem von $\varDelta_\varkappa$ nehmen, also die Functionaldeterminante mit $\varDelta_\varkappa$ einfach identificiren.

Setzen wir alle $f_\alpha = 0$, ausgenommen f_h und f_k, so wird dadurch zwischen $z_1, z_2, \cdots z_m$ eine einfache Mannigfaltigkeit bestimmt, die wir als die Linie $[hk]$ oder $[kh]$ je nach der Richtung, in der sie durchlaufen wird, bezeichnen wollen. Die Richtung stellen wir folgendermassen fest: Ist $(z_1, z_2, \cdots z_m)$ ein Punkt der Linie, dann werden die benachbarten Punkte auf ihr durch Incremente $(dz_1, dz_2, \cdots dz_m)$ bestimmt, für die das Gleichungssystem

$$\frac{\partial f_\alpha}{\partial z_1} dz_1 + \frac{\partial f_\alpha}{\partial z_2} dz_2 + \cdots + \frac{\partial f_\alpha}{\partial z_m} dz_m = 0$$
$$(\alpha = 0, 1, \cdots m \text{ ausser } h \text{ und } k)$$

gelten muss. Aus diesem Systeme linearer Gleichungen folgt

$$dz_1 : dz_2 : \cdots : dz_m = \frac{\partial^2 \varDelta}{\partial f_{k0} \partial f_{h1}} : \frac{\partial^2 \varDelta}{\partial f_{k0} \partial f_{h2}} : \cdots : \frac{\partial^2 \varDelta}{\partial f_{k0} \partial f_{hm}},$$

so dass gesetzt werden kann, wenn ε reell und unendlich klein genommen wird,

$$dz_\alpha = \pm \varepsilon^2 \frac{\partial^2 \varDelta}{\partial f_{k0} \partial f_{h\alpha}} = \mp \varepsilon^2 \frac{\partial^2 \varDelta}{\partial f_{h0} \partial f_{k\alpha}}.$$

*) Berl. Ber. 1869 März und August; 1878 Februar.

Hiernach giebt es zwei verschiedene Fortschrittsrichtungen; wir wollen die Curve bezeichnen mit

$$[hk] \text{ bei der Fortschrittsrichtung } dz_\alpha = \varepsilon^2 \frac{\partial^2 \Delta}{\partial f_{k0} \partial f_{h\alpha}};$$

$$[kh] \quad \text{"} \quad \text{"} \quad \text{"} \quad dz_\alpha = \varepsilon^2 \frac{\partial^2 \Delta}{\partial f_{h0} \partial f_{k\alpha}}.$$

§ 468. Wir untersuchen nun die Schnittpunkte von $[hk]$ mit $f_h = 0$. Ist $(\zeta_1, \cdots \zeta_m)$ ein Schnittpunkt, so wird $f_h(\zeta_1, \cdots \zeta_m) = 0$, und in dem benachbarten Punkte längs der Fortschrittsrichtung $[hk]$ hat f_h den Werth

$$\frac{\partial f_h}{\partial z_1} dz_1 + \cdots + \frac{\partial f_h}{\partial z_m} dz_m = \varepsilon^2 \left[\frac{\partial f_h}{\partial z_1} \frac{\partial^2 \Delta}{\partial f_{k0} \partial f_{h1}} + \cdots + \frac{\partial f_h}{\partial z_m} \frac{\partial^2 \Delta}{\partial f_{k0} \partial f_{hm}} \right]$$

$$= \varepsilon^2 \frac{\partial \Delta}{\partial f_{k0}} = \varepsilon^2 \Delta_k.$$

Daraus ersieht man: $[hk]$ tritt bei $(\zeta_1, \cdots \zeta_m)$ in das Innere von f_h, wenn Δ_k negativ ist, und in das Aeussere, wenn Δ_k positiv ist.

Wir nennen einen Punkt, in welchem $[hk]$ beim Passiren von $f_h = 0$ in den Binnenraum von (f_h, f_k) eintritt, einen Eintrittspunkt; einen Punkt, in welchem $[hk]$ beim Passiren von $f_h = 0$ aus dem Binnenraume von (f_h, f_k) heraustritt, einen Austrittspunkt von $[hk]$.

Es lässt sich leicht feststellen, wann $(\zeta_1, \zeta_2, \cdots \zeta_m)$ das Eine oder das Andere ist. Tritt $[hk]$ ins Innere von $f_h = 0$, und ist dabei $\operatorname{sgn} f_k(\zeta_1, \cdots \zeta_m) = +1$, so haben wir einen Eintrittspunkt; ebenso wenn $[hk]$ aus $f_h = 0$ heraustritt, und wenn dabei $\operatorname{sgn} f_k(\zeta_1, \cdots \zeta_m) = -1$ ist. In beiden Fällen wird $\operatorname{sgn} \Delta_k f_k = -1$.

Umgekehrt folgt für einen Austrittspunkt $\operatorname{sgn} \Delta_k f_k = +1$.

Wir setzen der Deutlichkeit halber noch die folgende Uebersicht her:

Eintrittspunkte.

$$\begin{array}{llll} \operatorname{sgn} f_h = +1,\ 0,\ -1; & \operatorname{sgn} f_h = -1,\ 0,\ +1 \\ \operatorname{sgn} f_k = \quad +1 \quad ; & \operatorname{sgn} f_k = \quad -1 \\ \operatorname{sgn} \Delta_k = \quad -1 \quad ; & \operatorname{sgn} \Delta_k = \quad +1 \end{array}$$

$$\operatorname{sgn} \Delta_k f_k = -1.$$

Austrittspunkte.

$$\begin{array}{llll} \operatorname{sgn} f_h = +1,\ 0,\ -1; & \operatorname{sgn} f_h = -1,\ 0,\ +1 \\ \operatorname{sgn} f_k = \quad -1 \quad ; & \operatorname{sgn} f_k = \quad +1 \\ \operatorname{sgn} \Delta_k = \quad -1 \quad ; & \operatorname{sgn} \Delta_k = \quad +1 \end{array}$$

$$\operatorname{sgn} \Delta_k f_k = +1.$$

Hieraus kann man eine Reihe wichtiger Schlüsse ziehen.

Auf einen Punkt $(\zeta_1, \cdots \zeta_m)$, in welchem $[hk]$ ins Innere von $f_h = 0$ tritt, folgt ein Schnittpunkt $(\zeta_1', \cdots \zeta_m')$ von $[hk]$ mit $f_h = 0$, in welchem $[hk]$ aus dem Inneren heraustritt, und umgekehrt. Im ersten ist Δ_k negativ, im zweiten positiv; da die Curve $[hk]$ geschlossen ist, weil alle $f_\alpha = 0$ ganz im Endlichen liegen, so wird

$$(1) \qquad \sum{}' \operatorname{sgn} \Delta_k = 0$$

(erstreckt auf alle Schnitte von $[hk]$ mit $f_h = 0$).

Bezeichnen wir die Anzahl der Male, in denen Eintrittspunkte bei $\operatorname{sgn} \Delta_k = -1$ auftreten, mit ε_1, und bei $\operatorname{sgn} \Delta_k = +1$ mit ε_2; ferner die Anzahl der Austrittspunkte bei $\operatorname{sgn} \Delta_k = -1$ mit α_1, und bei $\operatorname{sgn} \Delta_k = +1$ mit α_2, dann ist nach (1) und der obigen Tabelle

$$(2) \qquad \varepsilon_1 + \alpha_1 = \varepsilon_2 + \alpha_2.$$

§ 469. Verfolgen wir den Lauf von $[hk]$ und zählen die Eintrittspunkte und die Austrittspunkte in den Binnenraum von (f_h, f_k), die beim Schnitte mit $f_h = 0$ statthaben, dann ist die Gesammtzahl bei einem vollständigen Umlaufe eine gerade Zahl, $\varepsilon_1 + \varepsilon_2 + \alpha_1 + \alpha_2 \equiv 0$ (mod. 2), und also ist auch

$$(3) \qquad (\varepsilon_1 + \varepsilon_2) - (\alpha_1 + \alpha_2) = 2\chi$$

eine gerade Zahl. Die Hälfte derselben, also χ, nennen wir die Charakteristik des Systems der Functionen $f_0, f_1, \cdots f_m$; dazu sind wir berechtigt, weil, wie sich gleich zeigen wird, χ bei jeder Wahl von h und k denselben Werth besitzt.

Aus (3) in Verbindung mit (2) folgt sofort

$$(4) \qquad \chi = \varepsilon_1 - \alpha_2 = \varepsilon_2 - \alpha_1.$$

Infolge unserer Tabelle sehen wir, dass dies so ausgesprochen werden kann: Es ist

$$(5) \qquad \chi = \varepsilon_2 - \alpha_1 = \sum{}' \operatorname{sgn} \Delta_k,$$

wenn die Summe auf alle Punkte $(\zeta_1, \cdots \zeta_m)$ erstreckt wird, in denen

$$(5^a) \qquad f_k < 0; \;\; f_0 = 0, \cdots f_{k-1} = 0, \;\; f_{k+1} = 0, \cdots f_m = 0$$

ist; oder auch

$$(6) \qquad \chi = \varepsilon_1 - \alpha_2 = \sum{}' \operatorname{sgn} \Delta_k,$$

wenn die Summe auf alle Punkte $(\zeta_1, \cdots \zeta_m)$ erstreckt wird, in denen man hat:

$$(6^a) \qquad f_k > 0; \;\; f_0 = 0, \cdots f_{k-1} = 0, \;\; f_{k+1} = 0, \cdots f_m = 0.$$

Dafür können wir auch sagen: Die Charakteristik von f_0, $f_1, \cdots f_m$ ist gleich dem Ueberschuss der innerhalb $f_0 = 0$ liegenden Wurzeln von $f_1 = 0, \cdots f_m = 0$ mit $\operatorname{sgn} \varDelta_k = +1$ über diejenigen mit $\operatorname{sgn} \varDelta_k = -1$; oder gleich dem Ueberschuss der ausserhalb gelegenen mit $\operatorname{sgn} \varDelta_k = -1$ über diejenigen mit $\operatorname{sgn} \varDelta_k = +1$.

Bei dieser Darstellung von χ nimmt der Index h keine Ausnahmestellung mehr ein; man kann ihn daher mit jedem anderen vertauschen. Lässt sich also noch nachweisen, dass auch h und k untereinander vertauscht werden dürfen, dann ist die Constanz der Charakteristik nachgewiesen, denn man kann dann von $[hk]$ zu $[h'k]$, zu $[kh']$, zu $[k'h']$ und endlich zu $[h'k']$ übergehen, wobei h', k' zwei willkürliche Indices sind.

Dieser Theil des Beweises ist aber sehr einfach zu führen. Bezeichnen wir alle Eintritte der $[hk]$ in den Binnenraum von (f_h, f_k) sowohl beim Schnitte mit $f_h = 0$ als auch bei dem mit $f_k = 0$ der Reihe nach mit E', E'', E''', $\cdots$ und ebenso die Austritte mit A', A'', A''', $\cdots$ so ist, da auf jedes E ein A folgen muss und umgekehrt, die Summe der Anzahlen hier und da einander gleich. Die E', E'', $\cdots$ und die A', A'', $\cdots$ sind nun zunächst solche, bei denen f_h geschnitten wird; diese Anzahlen sind $(\varepsilon_1 + \varepsilon_2)$ und $(\alpha_1 + \alpha_2)$; und weiter solche, bei denen f_k geschnitten wird; diese Anzahlen seien e und a. Danach ist

$$e + (\varepsilon_1 + \varepsilon_2) = a + (\alpha_1 + \alpha_2),$$

$$2\chi = (\varepsilon_1 + \varepsilon_2) - (\alpha_1 + \alpha_2) = a - e. \tag{7}$$

Rechnet man, wie es die Regel vorschreibt, auf $[kh]$ die Eintritts- und die Austrittspunkte bei den Schnitten mit $f_k = 0$, so ist, da nun die umgekehrte Richtung gilt, jeder Punkt, der unter a vorkam, ein Eintrittspunkt und jeder, der unter e vorkam, ein Austrittspunkt; also zeigt (7) in Verbindung mit (3) die Richtigkeit des Theorems.

§ 470. Infolge der Tabelle können wir die Charakteristik noch anders deuten. Auf $[h0]$ ist $f_1 = 0, \cdots f_{h-1} = 0$, $f_{h+1} = 0, \cdots f_m = 0$; folglich wird in den Schnittpunkten von $[h0]$ mit $f_h = 0$ jedes f gleich Null ausser f_0. Jeder Schnittpunkt $(\zeta_1, \zeta_2, \cdots \zeta_m)$ ist also ein Wurzelpunkt für das System $f_\alpha = 0$ $(\alpha = 1, 2, \cdots m)$. Eintrittspunkte sind diejenigen unter ihnen, für welche $\operatorname{sgn} \varDelta_0 f_0 = -1$ ist, Austrittspunkte die, für welche $\operatorname{sgn} \varDelta_0 f_0 = +1$ ist. Die Charakteristik ist gleich dem doppelten Ueberschuss der Anzahl der Wurzelpunkte $(\zeta_1, \cdots \zeta_m)$, für welche $\operatorname{sgn} \varDelta_0 f_0 = -1$ über die, für welche $\operatorname{sgn} \varDelta_0 f_0 = +1$ wird.

Wenn man ferner statt der Function f_0 das Product $f_0 \Delta_0$ nimmt, dann ist die Charakteristik der Functionen

$$(\Delta_0 f_0, f_1, f_2, \cdots f_m)$$

gleich dem doppelten Ueberschuss der im Innern von $f_0 = 0$ gelegenen Punkte $(\zeta_1, \cdots \zeta_m)$ über die im Aeusseren gelegenen Punkte.

Wenn weiter der Bereich f_0 einen anderen Bereich g_0 vollständig einschliesst, so wird die Anzahl der zwischen beiden Umgrenzungen f_0 und g_0 gelegenen Punkte $(\zeta_1, \cdots \zeta_m)$ durch die Differenz der beiden Charakteristiken von

$$(\Delta_0 f_0, f_1, f_2, \cdots f_m) \quad \text{und von} \quad (\Delta_0 g_0, f_1, f_2, \cdots f_m)$$

gegeben.

Endlich können wir auch noch an die Stelle von $\operatorname{sgn} \Delta_k f_k$ setzen

$$\operatorname{sgn} \begin{vmatrix} f_0 & f_{01} & \cdots & f_{0m} \\ f_1 & f_{11} & \cdots & f_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ f_m & f_{m1} & \cdots & f_{mm} \end{vmatrix} = \operatorname{sgn} D,$$

da ja in jedem Schnittpunkte von $[hk]$ mit $f_k = 0$ alle f mit Ausnahme von f_k gleich Null werden. Ist also für ein $(\zeta_1, \cdots \zeta_m)$ das $\operatorname{sgn} D = -1$, so ist der Punkt ein Eintrittspunkt; ist $\operatorname{sgn} D$ gleich $+1$, so ist er ein Austrittspunkt. Folglich ist auch

$$(8) \qquad 2\chi = -\sum \operatorname{sgn} D$$

(erstreckt auf alle Punkte, in denen die $f = 0$ werden, ausser f_k).

Aus der Constanz der Charakteristik folgt, dass (8) denselben Werth besitzt, was auch immer für ein Index k genommen wird.

Die gleich im ersten Paragraphen dieser Vorlesung gemachte Annahme, dass alle $f = 0$ ganz im Endlichen verlaufen, ist für die gemachten Schlussfolgerungen eine wesentliche Voraussetzung, da ja alle Curven $[hk]$ geschlossene Curven sein müssen. Sobald man aber die Formel (5) anwendet, welche nur die Punkte im Innern von $f_k = 0$ benutzt, kann man die geschlossenen Theile der Curven $[hk]$, welche in $f_k > 0$ verlaufen, auch durch ungeschlossene Theile in $f_k > 0$ ersetzen; denn diese üben ja bei dieser Formel keinen Einfluss aus.

§ 471. Der Satz über die Constanz der als Charakteristik erklärten Zahl gehört in die Reihe der Theoreme der Lagen-Geometrie und muss als solcher rein anschauliche Beweise zulassen. Dies ist auch wirklich der Fall, wie wir jetzt zeigen wollen. Dabei benutzen wir den Inductionsschluss.

Es sei zunächst $m = 2$, und f_0, f_1, f_2 seien die gegebenen Functionen. Wir betrachten einen Binnenraum B von (f_1, f_2), der zwischen zwei aufeinanderfolgenden Schnittpunkten S_1 und S_2 von $f_1 = 0$, $f_2 = 0$ gelegen ist. Dabei mögen den $f_1 = 0$, $f_2 = 0$ beliebige Fortschrittsrichtungen zuertheilt sein. Dann hat S_1, als auf $f_1 = 0$ gelegen, einen bestimmten Charakter $\pi_1 = \pm 1$ hinsichtlich des Ein- oder Austrittes in (f_0, f_2); ebenso S_1, als auf $f_2 = 0$ gelegen, einen solchen $\pi_2 = \pm 1$ hinsichtlich (f_0, f_1). Nun wird $f_0 = 0$ die Begrenzung des Raumes B eine gerade Anzahl von Malen treffen; also ist die Zahl der Schnitte mit $f_1 = 0$ congruent der mit $f_2 = 0$ (mod. 2). Jeder zwischen S_1 und S_2 belegene Schnittpunkt auf f_1 ändert aber π_1; ähnliche Aenderung ruft jeder Schnittpunkt auf f_2 für π_2 hervor. Da beidemale die Zahl der Schnitte congruent (mod. 2) ist, so werden beide Charaktere gleichzeitig geändert, oder sie bleiben gleichzeitig ungeändert. Zählt man also die π in dieser Weise auf den ganzen Curven $f_1 = 0$ und auf $f_2 = 0$, so findet man gleiche absolute Werthe für χ, gleichgültig ob man auf $f_1 = 0$ oder auf $f_2 = 0$ die Zählung vornimmt. Giebt man also an einem beliebigen Schnittpunkte etwa S_1 den Curven $f_1 = 0$, $f_2 = 0$ solche Richtungen, dass $\pi_1 = \pi_2$ wird, dann sind die χ auf beiden Curven gerechnet auch unter Berücksichtigung des Vorzeichens identisch.

Nimmt man endlich $f_0 = 0$ mit $f_1 = 0$ zusammen, so folgt Gleiches; und daraus schliesst man dann, dass die Richtung, die dem f_0 ertheilt werden muss, unabhängig davon ist, ob man $f_1 = 0$ bei der Bestimmung derselben zu Hülfe nimmt, oder $f_2 = 0$. —

Für $(m + 1)$ Functionen $f_0, f_1, \cdots f_{m+1}$ kann man jetzt die Frage unmittelbar auf die für m Functionen zurückführen. Studirt man die Schnitte von $[hk]$ mit $f_h = 0$, $f_k = 0$, so reicht es aus aus, von der gesammten Figuration nur „die Schnitte" z. B. mit $f_0 = 0$ zu betrachten. Diese bilden genau die zu m Functionen gehörige Figur, nur in der Mannigfaltigkeit $f_0 = 0$ aufgefasst. Da sieht man dann sofort die Gültigkeit des allgemeinen Satzes ein.

§ 472. Wir wollen nun eine Anwendung der bisherigen allgemeinen Theorien geben.

Es sei $m = 2n$. Wir verstehen unter den F ganze reelle Functionen und setzen

$$F_\alpha(z_1 + iz_{n+1}, \cdots z_n + iz_{2n}) = f_\alpha(z_1, \cdots z_{2n}) + i f_{\alpha+n}(z_1, \cdots z_{2n})$$
$$(\alpha = 1, 2, \cdots n),$$

so dass die $f_1, f_2, \cdots f_{2n}$ reelle Functionen von $2n$ reellen Variablen sind. Nun ist

$$\frac{\partial F_\alpha}{\partial (z_\beta + i z_{n+\beta})} = \frac{\partial F_\alpha}{\partial z_\beta} = -i\frac{\partial F_\alpha}{\partial z_{n+\beta}} = \frac{\partial f_\alpha}{\partial z_\beta} + i\frac{\partial f_{\alpha+n}}{\partial z_\beta}$$
$$= -i\frac{\partial f_\alpha}{\partial z_{n+\beta}} + \frac{\partial f_{\alpha+n}}{\partial z_{n+\beta}},$$

und die Functionaldeterminante $\varDelta_0$ nimmt die Gestalt an

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \cdots \\ -a_{12} & a_{11} & -a_{14} & a_{13} & \cdots \\ a_{31} & a_{32} & a_{33} & a_{34} & \cdots \\ -a_{32} & a_{31} & -a_{34} & a_{33} & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Zur ersten Spalte addiren wir die zweite mit i multiplicirte; ebenso zur dritten die mit i multiplicirte vierte, u. s. w.; subtrahiren dann von der zweiten Zeile die mit i multiplicirte erste, von der vierten die mit i multiplicirte dritte, u. s. w. Hierdurch entsteht

$$\begin{vmatrix} a_{11} + i a_{12} & a_{12} & \cdots \\ 0 & a_{11} - i a_{12} & \cdots \\ a_{31} + i a_{32} & a_{32} & \cdots \\ 0 & a_{31} - i a_{32} & \cdots \\ \cdot & \cdot & \cdot \end{vmatrix};$$

addiren wir dann zur ersten Zeile die mit $\frac{1}{2i}$ multiplicirte zweite, u. s. f. und subtrahiren von der zweiten Spalte die mit $\frac{1}{2i}$ multiplicirte erste, u. s. f., dann bekommen wir

$$\begin{vmatrix} a_{11} + i a_{12} & 0 & \cdots \\ 0 & a_{11} - i a_{12} & \cdots \\ a_{31} + i a_{32} & 0 & \cdots \\ 0 & a_{31} - i a_{32} & \cdots \\ \cdot & \cdot & \cdot \end{vmatrix}$$
$$= \begin{vmatrix} a_{11} + i a_{12}, & \cdots \\ a_{31} + i a_{32}, & \cdots \\ \cdot & \cdot \end{vmatrix} \begin{vmatrix} a_{11} - i a_{12}, & \cdots \\ a_{31} - i a_{32}, & \cdots \\ \cdot & \cdot \end{vmatrix}.$$

Es ist also $\varDelta_0$ in diesem Falle die Summe zweier Quadrate und daher niemals negativ. Schon daraus ist ersichtlich, dass die Functionen f_α unseren Bedingungen nicht entsprechen. Denn es wird $\alpha_1 = \varepsilon_1 = 0$, und also nach (2) auch $\alpha_2 = \varepsilon_2 = 0$. Wir können uns aber auch direct davon überzeugen, dass jedes $f = 0$ sich ins Unendliche erstreckt. Geben wir den $z_2 + i z_{n+2}, \cdots z_n + i z_{2n}$ beliebige endliche feste

Werthe, und lassen den absoluten Betrag von $(z_1 + iz_{n+1})$ ins Unendliche wachsen, dann geht jedes F_α in ein $(A + Bi)(z_1 + iz_{n+1})^\varkappa$ über, wenn $\varkappa$ den höchsten vorkommenden Exponenten bedeutet. Es ist

$$(A + Bi)(z_1 + iz_{n+1})^\varkappa = (A + Bi)[U(z_1, z_{n+1}) + iV(z_1, z_{n+1})]$$
$$= (AU - BV) + i(BU + AV).$$

Die Gleichungen $U(t, 1) = 0$, $V(t, 1) = 0$ sind aber direct unter dem Biehler'schen Satze (§ 209, Bd. I) enthalten, und daraus folgt, dass sowohl sie selbst als auch, weil die Wurzeln von $U = 0$ und $V = 0$ sich gegenseitig trennen,

$$AU - BV = 0, \quad BU + AV = 0$$

reelle Wurzeln t haben; d. h. $f_\alpha = 0$ und $f_{\alpha+n} = 0$ erstrecken sich ins Unendliche.

Wir wollen weiter annehmen, dass die Glieder höchster Dimension in den f_α, gleich Null gesetzt, kein Gleichungssystem mit gemeinsamen Wurzeln ergeben. Dann kann man für die absoluten Beträge der $z_1, \cdots z_{2n}$ eine Grenze ϱ_0 angeben, oberhalb deren das System $f_\alpha = 0$ keine Wurzel mehr besitzt. Um dies zu zeigen, setzen wir

$$z_1 = \varrho u_1, \; z_2 = \varrho u_2, \cdots z_{2n} = \varrho u_{2n} \qquad (\Sigma u^2 = 1)$$

und nach Dimensionen geordnet

$$f_\alpha(z_1, \cdots z_{2n}) = \varrho^{\varkappa_\alpha} \varphi_\alpha(u_1, \cdots u_{2n}) + \varrho^{\varkappa_\alpha - 1} \psi_\alpha(u_1, \cdots u_{2n}) + \cdots.$$

Dann haben die $\varphi_\alpha = 0$ kein gemeinsames Wurzelsystem u, und also sinkt $\sum \varphi_\alpha^2$ nicht unter einen endlichen positiven Werth. Bilden wir also

$$\left| \frac{f_\alpha(z_1, \cdots z_{2n})}{\varrho^{\varkappa_\alpha}} \right|^2 = \sum \varphi_\alpha^2 + \frac{1}{\varrho} \Psi_1 + \frac{1}{\varrho^2} \Psi_2 + \cdots,$$

so kann das erste Glied rechts nicht unter einen endlichen positiven Werth abnehmen. Für $\Psi_1, \Psi_2, \cdots$ kann man leicht obere Grenzen angeben, indem man alle $u = 1$ setzt und alle Coefficienten durch die grössten absoluten Werthe ersetzt, die sie erreichen dürfen. Danach lässt sich dann ϱ_0 so bestimmen, dass für $\varrho \geqq \varrho_0$ die rechte Seite von Null verschieden bleibt, und ϱ_0 ist somit die gewünschte Grenze.

Nehmen wir also ein $f_0(z_1, \cdots z_{2n}) = 0$, welches ganz im Aeusseren der Fläche $\Sigma z_\lambda^2 - \varrho_0^2 = 0$ verläuft, so können wir, ohne die Wurzelanzahl von $f_1 = 0, \cdots f_{2n} = 0$ innerhalb $f_0 = 0$ zu beeinflussen, alle $f_1, \cdots$ ausserhalb $f_0 = 0$ durch geschlossene Stücke ersetzt denken.

Dann erst gelten die Formeln (5), (5ᵃ) für $k = 0$, da sie sich nur auf Configurationen innerhalb des Gebietes $f_0 = 0$ beziehen. Das

Ergebniss, dass $\Delta_0 > 0$ ist, gilt also auch nur für sie. In $f_0 < 0$ giebt es daher nur Eintrittspunkte, d. h. die Charakteristik $\chi = \varepsilon_2$ giebt direct die Anzahl der Schnittpunkte von $f_1 = 0, \cdots f_{2n} = 0$.

Wir wollen jetzt die Beschaffenheit der durch

$$f_1 = 0, \cdots f_{h-1} = 0, \quad f_{h+1} = 0, \cdots f_{2n} = 0$$

auf f_0 herausgeschnittenen Punkte untersuchen. Geht man auf $[h0]$ vom Aeusseren $f_0 > 0$ kommend beim Punkte P in das Gebiet $f_1 < 0$ hinein, und trifft man auf $[h0]$ bei Q den ersten Schnittpunkt von $[h0]$ mit $f_h = 0$, so muss, da Q ein Eintrittspunkt ist, nach der Tabelle f_h vom Negativen ins Positive gehen; folglich liegt P im Bereiche $f_h < 0$, und da $[0h]$ die entgegengesetzte Richtung hat, so tritt $[0h]$ bei P aus $f_0 < 0$ in $f_0 > 0$, d. h. P ist auf $[0h]$ ein Eintrittspunkt.

Geht man ferner auf $[h0]$ vom Inneren $f_0 < 0$ kommend beim Punkte S aus dem Gebiete $f_0 < 0$ heraus, und ist R der letzte vorhergehende Schnittpunkt von $[h0]$ mit $f_h = 0$, so ist auch hier wieder, da R ein Eintrittspunkt ist, $[h0]$ aus $f_h < 0$ in $f_h > 0$ getreten, und S liegt deshalb in $f_h > 0$. Deshalb tritt $[0h]$ bei S in der Richtung RS betrachtet innerhalb $f_h > 0$ aus $f_0 > 0$ in $f_0 < 0$; S ist also nach der Tabelle ein Eintrittspunkt. Folglich giebt es auf $f_0 = 0$ an Schnitten mit einem beliebigen Systeme von $(2n - 1)$ der $f = 0$ nur Eintrittspunkte. Nun ist die Anzahl derselben gleich 2χ. Also folgt: Innerhalb $f_0 = 0$ und ebenso auf $f_0 = 0$ giebt es nur Eintrittspunkte, und zwar liegen auf $f_0 = 0$ doppelt so viel Schnittpunkte mit jeder durch Ausschluss einer der übrigen Functionen f_λ gebildeten Linien, als im Inneren Schnittpunkte der $f_1, f_2, \cdots$ vorhanden sind.

§ 473. Wir kehren zu dem allgemeinen Falle willkürlicher f_0, $f_1, \cdots f_m$ zurück, die nur den oben aufgestellten Bedingungen zu genügen haben. Gehen wir durch Variation der Constanten von jenem ersten Systeme zu einem zweiten über, so kann die Variation stets so vorgenommen werden, dass man zunächst eine der Functionen in die neue Form überführt, während die übrigen ungeändert bleiben; dann mit einer zweiten ebenso verfährt, u. s. f. Auf diese Weise kann man am Einfachsten übersehen, wie die Charakteristik des Systems sich ändert. Nach Formel (5) ist $\chi = \sum \operatorname{sgn} \Delta_k$, ausgedehnt über die Stellen, an denen alle $f_\alpha = 0$ sind, ausgenommen f_k, welches negativ ist. Bei festen f_α und variirtem f_k kann in jenem Ausdrucke, in welchem ja dann auch Δ_k für jedes System $(\zeta_1, \cdots \zeta_m)$ constant ist, χ sich nur dann ändern, wenn einer der Punkte $(\zeta_1, \cdots \zeta_m)$ bei der Variation von f_k aus dem Gebiete $f_k < 0$ in das Gebiet $f_k > 0$ tritt, oder umgekehrt.

Dabei muss das Gebilde $f_k = 0$ den Punkt $(\zeta_1, \cdots \zeta_m)$ überschritten haben, d. h. es müssen gleichzeitig alle $(m+1)$ Functionen $f_\varkappa$ gleich Null geworden sein. Da Gleiches für alle anderen Functionen gilt, so haben wir den Satz: Die Charakteristik kann bei Variation der Functionen f nur dann eine Aenderung erfahren, wenn ein System von Functionen passirt wird, welche sämmtlich für ein und dasselbe Werthsystem $(\zeta_1, \cdots \zeta_m)$ verschwinden. Jenachdem dabei

$$|f_{\varkappa\lambda}| \qquad (\varkappa, \lambda = 0, 1, \cdots m;\ f_{\varkappa 0} = f_\varkappa)$$

aus dem Positiven ins Negative übergeht oder umgekehrt, nimmt die Charakteristik um eine Einheit zu oder ab, wenn nicht etwa die passirte Stelle singulär ist.

§ 474. Nach diesen Resultaten ändert sich in unserem Beispiele von § 472 die Charakteristik nicht, wenn wir bei hinreichend hoch gewähltem ϱ_0 die Coefficienten der f um endliche Grössen variiren, die einen gegebenen Betrag nicht überschreiten. Da in diesem Falle die Charakteristik zugleich die Anzahl der Wurzeln der Gleichungen

$$F_\alpha(z_1 + iz_{n+1}, \cdots z_n + iz_{2n}) = 0 \qquad (\alpha = 1, 2, \cdots n)$$

ergiebt, so bleibt auch sie ungeändert, wenn man die Functionen für $\alpha = 1, 2, \cdots (n-1)$ auf ihre Glieder höchster Dimensionen beschränkt. Liefern dann diese homogenen Gleichungen q Werthsysteme für die Verhältnisse der $(z_\alpha + iz_{\alpha+n})$ untereinander, und trägt man diese in die letzte Gleichung ein, deren Dimension t sein mag, so folgt sofort, dass das System der $F_\alpha = 0$ genau qt Wurzeln besitzt. Ist der Bézout'sche Satz also für $(n-1)$ Gleichungen schon bewiesen, so gilt er hiernach auch für n Gleichungen.

Im Falle $n = 1$ genügt es, die Function F_1 in $(z_1 + iz_2)^t + a = 0$ zu verwandeln, um direct zu dem Fundamentaltheorem der Theorie der algebraischen Gleichungen zu gelangen. Hierdurch wird das eigentliche Wesen des vierten Gauss'schen Beweises dargelegt, indem gezeigt wird, dass für die zwei durch irgend eine algebraische Gleichung $F_1(z_1 + iz_2) = 0$ dargestellten Curvensysteme $f = 0$ die Configuration in Bezug auf deren Schnittpunkte innerhalb eines hinreichend gross gewählten Kreises nicht anders ist, wie für diejenigen Curvensysteme, welche aus einer binomischen Gleichung desselben Grades hervorgehen. Man kann es übrigens an Gauss' Deductionen selbst erkennen, dass dabei eigentlich nur die höchste Potenz von $(z_1 + iz_2)$ und von den Coefficienten der übrigen Glieder der Gleichung nur die Eigenschaft in Betracht gezogen wird, dass ihre absoluten Werthe unter einer

gewissen Grenze liegen, so dass eine dabei zulässige Veränderung der Coefficienten die Deduction nicht berührt*).

§ 475. In engem Zusammenhange mit dieser Theorie steht eine Erweiterung der früher behandelten (Vorles. 20; § 228 ff., Bd. I) Theoreme von Hermite, welche dieser selbst angedeutet hat**). Die hierzu nöthigen Erwägungen sind nicht sehr von jenen früheren verschieden, so dass wir kürzer sein und gleich, von allgemeinen Formeln absehend, die interessantesten und wichtigsten Specialfälle behandeln können.

Die m Gleichungen

$$f_\alpha(z_1, z_2, \cdots z_m) = 0 \qquad (\alpha = 1, 2, \cdots m) \tag{9}$$

zwischen den m Unbekannten $z_1, \cdots z_m$ mögen k endliche Wurzeln $(\zeta_{1\varrho}, \zeta_{2\varrho}, \cdots \zeta_{m\varrho})$ haben, $\varrho = 1, 2, \cdots k$, deren Anzahl nicht nothwendig gleich dem Producte der Dimensionen von $f_1, f_2, \cdots$ ist. Bei diesen Wurzeln können einige Coordinaten reell, andere complex sein; unter einer reellen Wurzel verstehen wir eine solche, die nur reelle Coordinaten hat; conjugirt complexe Wurzeln sind solche von einander verschiedene Wurzeln, von denen jede in die andere übergeht, wenn man in allen Coordinaten $+i$ durch $-i$ ersetzt. Bei Gleichungen mit reellen Coordinaten kommen conjugirt complexe Wurzeln gleichzeitig vor.

Wir nehmen als Unbestimmte einer quadratischen Form $u_0, u_1, \cdots u_{k-1}$ an, bezeichnen mit $\psi(z_1, \cdots z_m; t)$ eine ganze Function der z und des t, welche bei unbestimmtem t für keine Wurzel $(\zeta_{1\varrho}, \cdots \zeta_{m\varrho})$ verschwindet, und mit $\varpi(z_1, \cdots z_m)$ eine ganze Function der z, welche für alle k Wurzeln voneinander verschiedene Werte annimmt; dann setzen wir

$$\begin{aligned} \varphi(u, t) &= \sum_{\varrho=1}^{k} \psi(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}; t)[u_0 + \varpi(\zeta_{1\varrho}, \cdots)u_1 + \cdots + \varpi^{k-1}(\zeta_{1\varrho}, \cdots)u_{k-1}]^2 \\ &= \sum_{\alpha, \beta=0}^{k-1} u_\alpha u_\beta \sum_{\varrho=1}^{k} \psi(\zeta_{1\varrho}, \cdots; t)\, \varpi^{\alpha+\beta}(\zeta_{1\varrho}, \cdots). \end{aligned} \tag{10}$$

Zur Bestimmung des Ranges dieser quadratischen Form (§ 166, Bd. I) und zugleich, um sie in ein Aggregat von Quadraten zu verwandeln, bilden wir für $q = k, k-1, \cdots 1$ die symmetrische Summe

$$\varDelta_q = S(\psi(\zeta_{11}, \cdots; t) \cdots \psi(\zeta_{1q}, \cdots; t)) \begin{vmatrix} 1 & \varpi(\zeta_{11}, \cdots) \cdots \varpi^{q-1}(\zeta_{11}, \cdots) \\ \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \\ 1 & \varpi(\zeta_{1q}, \cdots) \cdots \varpi^{q-1}(\zeta_{1q}, \cdots) \end{vmatrix}^2; \tag{11}$$

*) Kronecker, l. c., 1878 Febr., p. 151.

**) C. R. 36 (1859), p. 294.

insbesondere wird

$$(11^a)\qquad \Delta_k' = \prod_{\varrho=0}^{k} \psi(\zeta_{1\varrho}, \cdots; t) \prod_{\alpha,\beta} [\varpi(\zeta_{1\alpha}, \cdots) - \varpi(\zeta_{1\beta}, \cdots)]^2;$$

dies ist nach unseren Voraussetzungen von Null verschieden; also ist φ vom Range k, d. h. in eine Summe von nicht weniger als k Quadraten transformirbar. Eine solche Darstellung wird im regulären Falle

$$(12)\qquad \varphi = \frac{1}{\Delta_1} \chi_1^2 + \frac{1}{\Delta_1 \Delta_2} \chi_2^2 + \cdots + \frac{1}{\Delta_{k-1}\Delta_k} \chi_k^2.$$

Kommt es darauf an, die Δ als von t abhängig zu kennzeichnen, dann schreiben wir $\Delta_1(t)$, $\Delta_2(t)$, $\cdots$.

Die Signatur von φ wird dabei durch die Differenz der Anzahl der positiven und der negativen Coefficienten, $P(t)$ und $N(t)$, in (12) bestimmt; bezeichnen wir sie mit $S(t)$, so ist

$$P(t) - N(t) = S(t); \quad P(t) + N(t) = k.$$

Es bleibt $S(t)$ von der Art der Darstellung der Form φ als Aggregat von Quadraten unabhängig. Genau wie in § 229, Bd. I folgt daher: Die Signatur von $\varphi(u, t)$ ist

$$(13)\qquad S(t) = \sum_{\varrho} \operatorname{sgn} \psi(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}; t)$$

(erstreckt über alle reellen Wurzeln der $f_\alpha = 0$).

$P(t)$ ist die Summe aus der Anzahl der Paare complexer Wurzeln und der Anzahl der reellen, für die $\operatorname{sgn}\psi = +1$ ist; $S(t)$ die Summe aus der Anzahl der Paare complexer Wurzeln und der Anzahl der reellen, für die $\operatorname{sgn}\psi = -1$ ist.

Ist $t_2 > t_1$, dann giebt

$$P(t_1) - P(t_2)$$

den Ueberschuss der Anzahl reeller Wurzeln, für die $\operatorname{sgn}\psi(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}; t_1) = 1$ ist, über die Anzahl derjenigen, für die $\operatorname{sgn}\psi(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}; t_2) = 1$ wird.

§ 476. Wir tragen zunächst $\psi = 1$ in (10) ein. Dadurch wird

$$\varphi = \sum u_\alpha u_\beta S_{\alpha+\beta}, \quad \Delta_\lambda = |S_{\mu+\nu}| \qquad (\mu, \nu = 0, 1, \cdots \lambda - 1),$$

falls wir unter $S_\varkappa$ die Summe der $\varkappa^{\text{ten}}$ Potenzen aller Werthe von $\omega(\zeta_{1\varrho}, \cdots)$ verstehen. Hier ist stets $\operatorname{sgn}\psi = +1$; folglich wird nach (13) S gleich der Anzahl aller reellen Wurzeln, d. h.: Die Anzahl der reellen Wurzeln ist $P - N$, wobei P die Anzahl der Zeichenfolgen, N diejenige der Zeichenwechsel in

$$1, \Delta_1, \Delta_2, \cdots \Delta_k$$

bedeutet. Es ist dies genau derselbe Satz, der für eine Variable abgeleitet wurde. —

An zweiter Stelle setzen wir

$$\begin{aligned} \psi(z_1, \cdots z_m; t_1) &= (z_1 - a_1)(z_2 - a_2) \cdots (z_m - a_m), \\ \psi(z_1, \cdots z_m; t_2) &= (z_1 - b_1)(z_1 - b_2) \cdots (z_m - b_m), \end{aligned} \quad (t_2 > t_1),$$

wobei jedes a_k kleiner als das entsprechende b_k sein soll. Dann giebt $P(t_1) - P(t_2)$ den Ueberschuss der Anzahl der Wurzeln, für welche

$$(\zeta_{1\varrho} - a_1)(\zeta_{2\varrho} - a_2) \cdots (\zeta_{m\varrho} - a_m) > 0$$

ist, über die Anzahl derer, für welche

$$(\zeta_{1\varrho} - b_1)(\zeta_{1\varrho} - b_2) \cdots (\zeta_{m\varrho} - b_m) > 0$$

wird. Um dieses Resultat weiter ausnützen zu können, müssen wir folgende Betrachtungen anstellen, die ihrer Natur nach in die Geometrie der Lage gehören.

Es seien in einem m-fach ausgedehnten Raume $z_1, z_2, \cdots z_m$ die m Coordinaten eines Punktes; ferner seien a_1 und b_1 $(> a_1)$ zwei Specialwerthe von z_1, ebenso a_2 und b_2 $(> a_2)$ zwei solche von z_2 u. s. f. Es soll ferner γ_1 einen der beiden Werthe a_1, b_1 bezeichnen, γ_2 einen der beiden Werthe a_2, b_2 u. s. f. Dann gilt es 2^m Ausdrücke

$$\psi = (z_1 - \gamma_1)(z_2 - \gamma_2) \cdots (z_m - \gamma_m),$$

je nach der Wahl der einzelnen γ.

Ferner sei $(\zeta_{1\varrho}, \zeta_{2\varrho}, \cdots \zeta_{m\varrho})$ für $\varrho = 1, 2, \cdots$ eine willkürliche Zahl von willkürlich im Raume vertheilten Punkten, wobei nur kein $\zeta_{\alpha\varrho}$ mit a_α und b_α zusammenfallen soll. Wir bilden alle

$$\operatorname{sgn} \psi(\zeta_{1\varrho}, \zeta_{2\varrho}, \cdots \zeta_{m\varrho}; \gamma_1, \gamma_2, \cdots \gamma_m),$$

behalten nur die positiven bei und multipliciren ein jedes dieser sgn mit $+1$ oder -1, jenachdem unter den $\gamma_1, \gamma_2, \cdots \gamma_m$ eine gerade oder eine ungerade Anzahl von Werthen b vorkommt. Die Summe

$$\frac{1}{2^{m-1}} \sum_{(\gamma)} \pm \operatorname{sgn} \psi(\zeta_{1\varrho}, \cdots \zeta_{m\varrho}; \gamma_1, \cdots \gamma_m) \tag{14}$$

erstreckt über alle 2^m Combinationen der γ ist gleich der Anzahl derjenigen Punkte $(\zeta_{1\varrho}, \cdots \zeta_{m\varrho})$, für welche

$$a_1 < \zeta_{1\varrho} < b_1, \quad a_2 < \zeta_{2\varrho} < b_2, \cdots a_m < \zeta_{m\varrho} < b_m) \tag{15}$$

wird. Um diesen Satz zu beweisen, nehmen wir irgend ein ψ, dessen $\operatorname{sgn} = +1$ ist. In ihm möge etwa $\zeta_{1\varkappa} < a_\varkappa$ oder auch $\zeta_{1\varkappa} > b_\varkappa$ sein. Dann ändert sich das sgn nicht, wenn man den vorkommenden Werth $a_\varkappa$ oder $b_\varkappa$ von $\gamma_\varkappa$ durch den anderen $b_\varkappa$ oder $a_\varkappa$ ersetzt, wohl aber ändert sich das Vorzeichen vor dem sgn; beide Glieder der Summe zerstören

sich also. Ebenso ordnen sich alle anderen, bei denen mindestens ein $\zeta_{1\varkappa} < a_\varkappa$ oder $> b_\varkappa$ ist, zu je zweien einander zu, die sich zerstören. Es bleiben also nur die Punkte zurück, deren Coordinaten sämmtlich den Bedingungen (15) genügen. Hier ist $(z_1 - a_1)\cdots(z_m - a_m)$ positiv, und ebenso jedes Product, bei dem eine gerade Anzahl der a durch die entsprechenden b ersetzt ist. Alle erhalten ein $+$ Zeichen vor das sgn. Es sind also die einzigen, die in (14) zählen; solcher giebt es 2^{m-1}, nämlich $1 + \binom{m}{2} + \binom{m}{4} + \cdots$; und damit ist der Satz bewiesen.

Setzen wir nun direct unser jetziges ψ in die obigen Formeln ein, so erhalten wir den Satz: Die Anzahl aller Wurzeln von (9), welche die Bedingungen (15) befriedigen, wird durch die Anzahl (14) geliefert.

Für $m = 2$ und $m = 3$ stellt sich dies folgendermassen: Verwandelt man

$$\varphi = \sum_{\varrho=1}^{k} (\zeta_{1\varrho} - \gamma_1)(\zeta_{2\varrho} - \gamma_2)[u_0 + \varpi(\zeta_{1\varrho}, \zeta_{2\varrho})u_1 + \cdots + \varpi^{k-1}(\zeta_{1\varrho}, \zeta_{2\varrho})u_{k-1}]^2$$

in eine Summe von Quadraten und bezeichnet mit $P(\gamma_1, \gamma_2)$ die Anzahl der positiven Summanden, dann giebt

$$\frac{1}{2}[P(a_1, a_2) - P(a_1, b_2) - P(b_1, a_2) + P(b_1, b_2)]$$

die Anzahl derjenigen reellen Wurzeln von $f_1 = 0$, $f_2 = 0$, welche in dem Rechtecke mit den Ecken (a_1, a_2); (a_1, b_2); (b_1, a_2); (b_1, b_2) liegen. —

Verwandelt man

$$\varphi = \sum_{\varrho=1}^{k} (\zeta_{1\varrho} - \gamma_1)(\zeta_{2\varrho} - \gamma_2)(\zeta_{3\varrho} - \gamma_3)[u_0 + \cdots + \varpi^{k-1}(\zeta_{1\varrho}, \zeta_{2\varrho}, \zeta_{3\varrho})u_{k-1}]^2$$

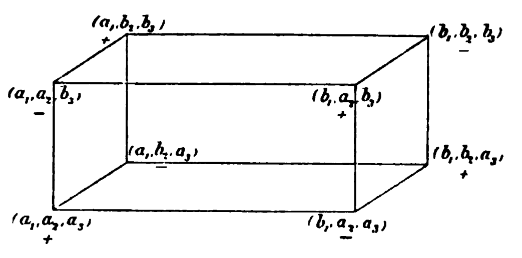
in eine Summe von Quadraten und bezeichnet mit $P(\gamma_1, \gamma_2, \gamma_3)$ die Anzahl der positiven Glieder unter ihnen, dann giebt

$$\frac{1}{4}[P(a_1, a_2, a_3) - P(a_1, a_2, b_3) - P(a_1, b_2, a_3) - P(b_1, a_2, a_3) + P(a_1, b_2, b_3) + P(b_1, a_2, b_3) + P(b_1, b_2, a_3) - P(b_1, b_2, b_3)]$$

die Anzahl derjenigen reellen Wurzeln von

$$f_1 = 0,\quad f_2 = 0,\quad f_3 = 0,$$

welche in dem Parallelepipedon mit den Ecken



$$(a_1, a_2, a_3), \quad (a_1, a_2, b_3), \quad (a_1, b_2, a_3), \quad (b_1, a_2, a_3),$$
$$(a_1, b_2, b_3), \quad (b_1, a_2, b_3), \quad (b_1, b_2, a_3), \quad (b_1, b_2, b_3)$$

liegen.

§ 477. Wir können auch die allgemeine Form (10) direct zu den Untersuchungen über die Charakteristik von Functionensystemen in Beziehung setzen. Trägt man nämlich statt $\psi(z_1, \cdots z_m; t)$ in (10) und in (13) ein $f_0 \Delta_0$, wo Δ_0 die gleiche Bedeutung hat, wie in den ersten Paragraphen dieser Vorlesung, dann zeigt (13), dass die Signatur S den Ueberschuss derjenigen Wurzeln von $f_\alpha = 0$, für welche $\operatorname{sgn} f_0 \Delta_0 = -1$ ist, über diejenigen angiebt, für welche $\operatorname{sgn} f_0 \Delta_0 = +1$ ist. Nach § 470 hat dies den Werth der halben Charakteristik des Functionensystems $f_0, f_1, \cdots f_m$. Es gilt demnach die Gleichung

$$2\chi = P - N,$$

durch welche die Bestimmung der Charakteristik eines Functionensystems auf die Untersuchung einer quadratischen Form reducirt wird. Hierdurch wird also eine wesentliche Lücke, die bei unserer Darstellung der Kronecker'schen Theorie offen blieb, in einfacher Weise durch die Hermite'schen Betrachtungen ausgefüllt.

Siebenundvierzigste Vorlesung.

Die Auflösung linearer Gleichungen.

§ 478. Wir wollen als Anhang zu der Theorie mehrerer Gleichungen mit mehreren Unbekannten den einfachen Fall linearer Gleichungen behandeln. Das erscheint deshalb nicht unangebracht, weil noch vielfach in Lehrbüchern dieser Gegenstand nicht in der möglichen Kürze dargestellt wird, deren er fähig ist, und ferner, weil die mitunter gewählte Reduction der Frage auf homogene Gleichungen den Kernpunkt der Sache insofern verschiebt, als die Erkenntniss der Bedingungen für die Existenz endlicher Lösungen verhüllt und verhindert wird.

Es sei ein System constanter Grössen a_{ik} gegeben ($i = 1, 2, \cdots p$; $k = 1, 2, \cdots q$), welche in p Zeilen und q Spalten angeordnet sind; r sei die grösste Zahl, für welche nicht alle Determinanten verschwinden, deren Elemente durch die Schnitte von r Zeilen und r Spalten des Systems geliefert werden. Dann heisst r der Rang des Systems*).

*) Kronecker, Berl. Ber. 1884 Dec., § 5.

Wir können durch Vertauschung von Spalten untereinander und von Zeilen untereinander die Elemente so angeordnet denken, dass die Determinante

(1) $$D = |a_{ik}| \qquad (i, k = 1, 2, \cdots r)$$

eine der von Null verschiedenen Determinanten r^{ter} Ordnung des Systems wird.

Nun mögen p lineare Functionen gegeben sein

(2) $$f_\alpha \equiv a_{\alpha 1} z_1 + a_{\alpha 2} z_2 + \cdots + a_{\alpha q} z_q \qquad (\alpha = 1, 2, \cdots p),$$

über deren Anzahl p hinsichtlich der Beziehung zur Anzahl q der z keinerlei Voraussetzungen gemacht werden. Es ist jede Determinante

(3) $$| f_\varkappa \;\; a_{\varkappa 1} \;\; a_{\varkappa 2} \cdots a_{\varkappa r} | \equiv 0 \qquad (\varkappa = \alpha, 1, 2, \cdots r).$$

Denn trägt man (2) ein, so wird jedes z mit einer Determinante $(r+1)^{\text{ter}}$ Ordnung der a_{ik} multiplicirt auftreten; diese verschwindet, da das System a_{ik} den Rang r hat. Ferner ist in (3) der Coefficient von f_α gleich D und also von Null verschieden. Man erhält durch Entwickelung die für jedes System $z_1, \cdots z_q$ geltenden Gleichungen

(3ᵃ) $$D f_\alpha + D_{\alpha 1} f_1 + D_{\alpha 2} f_2 + \cdots + D_{\alpha r} f_r = 0 \qquad (\alpha = 1, 2, \cdots p),$$

vermittels deren man im Stande ist, jede der Functionen $f_1, f_2, \cdots f_p$ durch die r ersten unter ihnen linear und homogen auszudrücken.

§ 479. Sind demnach die p Gleichungen vorgelegt

(4) $$f_1 + a_{10} = 0, \; f_2 + a_{20} = 0, \cdots f_p + a_{p0} = 0,$$

so sind diese wegen (3) nur dann lösbar, wenn alle

$$| a_{\varkappa 0} \;\; a_{\varkappa 1} \;\; a_{\varkappa 2} \cdots a_{\varkappa r} | \equiv 0 \qquad (\varkappa = \alpha, 1, 2, \cdots r)$$

sind, d. h. nur dann, wenn das System

(5) $$| a_{gh} | \qquad (g = 1, 2, \cdots p; \; h = 0, 1, 2, \cdots q)$$

von dem gleichen Range ist wie

(5ᵃ) $$| a_{ik} | \qquad (i = 1, 2, \cdots p; \; k = 1, 2, \cdots q).$$

Wir wollen annehmen, es wäre (5) vom Range r. Dann bilden wir die Gleichung, deren Richtigkeit für unbestimmte z nun feststeht,

(3ᵇ) $$D(f_\alpha + a_{\alpha 0}) + D_{\alpha 1}(f_1 + a_{10}) + \cdots + D_{\alpha r}(f_r + a_{r0}) = 0$$

und entnehmen aus ihr, dass wenn die r ersten Gleichungen

(4ᵃ) $$f_1 + a_{10} = 0, \cdots f_r + a_{r0} = 0$$

erfüllt sind, alle übrigen von selbst befriedigt werden. Wir können also das System (4) jetzt durch (4ᵃ) ersetzen.

Werden die Gleichungen (4ᵃ) durch gewisse Werthe der z befriedigt, dann wird für diese Werthe z

$$|f_\varkappa + a_{\varkappa 0},\ a_{\varkappa 2}, \cdots a_{\varkappa r}| = 0 \qquad (\varkappa = 1, 2, \cdots r).$$

Subtrahirt man hier die zweite mit z_2 multiplicirte Spalte von der ersten, die dritte mit z_3 multiplicirte ebenfalls, u. s. w., dann entsteht

$$|a_{\varkappa 1} z_1 + a_{\varkappa, r+1} z_{r+1} + \cdots + a_{\varkappa, q} z_q + a_{\varkappa 0},\ a_{\varkappa 2}, \cdots a_{\varkappa r}| = 0$$
$$(\varkappa = 1, 2, \cdots r),$$

oder entwickelt

$$D \cdot z_1 + \varDelta_{10} + \varDelta_{1, r+1} z_{r+1} + \varDelta_{1, r+2} z_{r+2} + \cdots + \varDelta_{1, q} z_q = 0,$$

und auf ähnliche Weise erhält man

$$(6) \quad D \cdot z_\alpha + \varDelta_{\alpha 0} + \varDelta_{\alpha, r+1} z_{r+1} + \varDelta_{\alpha, r+2} z_{r+2} + \cdots + \varDelta_{\alpha, q} z_q = 0$$
$$(\alpha = 1, 2, \cdots r).$$

Diese Gleichungen bestimmen $z_1, z_2, \cdots z_r$ durch die willkürlich gebliebenen Grössen $z_{r+1}, z_{r+2}, \cdots z_q$.

Endlich ist auch noch die Umkehrung zu beweisen, dass durch alle Werthsysteme z, welche den Gleichungen (6) genügen, auch alle Gleichungen (4^a) befriedigt werden. Dazu schreiben wir (6) etwas ausführlicher in der Form

$$D z_\alpha + \sum_{\beta=1}^{q-r} z_{r+\beta} \left(a_{1, r+\beta} \frac{\partial D}{\partial a_{1\alpha}} + \cdots + a_{r, r+\beta} \frac{\partial D}{\partial a_{r\alpha}} \right)$$
$$+ \left(a_{10} \frac{\partial D}{\partial a_{1\alpha}} + \cdots + a_{r0} \frac{\partial D}{\partial a_{r\alpha}} \right) = 0.$$

Wir multipliciren diese Gleichung mit $a_{\varrho\alpha}$, wobei ϱ eine der Zahlen $1, 2, \cdots r$ sein soll, und summiren über $\alpha = 1, 2, \cdots r$. Dabei wird der Coefficient von $z_{r+\beta}$

$$a_{1, r+\beta} \left[a_{\varrho 1} \frac{\partial D}{\partial a_{11}} + a_{\varrho 2} \frac{\partial D}{\partial a_{12}} + \cdots \right]$$
$$+ a_{2, r+\beta} \left[a_{\varrho 1} \frac{\partial D}{\partial a_{21}} + a_{\varrho 2} \frac{\partial D}{\partial a_{22}} + \cdots \right] + \cdots.$$

Offenbar verschwinden alle eckigen Klammern mit Ausnahme der einen, welche $a_{\varrho, r+\beta}$ zum Factor hat, und diese nimmt den Werth D an. Hierdurch geht die angegebene Summe in

$$D \cdot (a_{\varrho 1} z_1 + a_{\varrho 2} z_2 + \cdots + a_{\varrho q} z_q + a_{\varrho 0}) = 0$$

über, und also, weil $D \neq 0$ ist, in $f_\varrho = 0$. Es sind demnach alle Gleichungen (4^a) wirklich befriedigt, und die Formeln (6) geben die allgemeine Lösung von (4).

§ 480. Im Falle homogener Gleichungen gilt $a_{\varrho 0} = 0$; die Bedingung, dass (5) von gleichem Range mit (5^a) sein soll, ist deswegen stets von selbst erfüllt. Ferner wird in (6) $\varDelta_{\alpha 0} = 0$ zu setzen sein.

Ist dann $q = r$, d. h. die Anzahl der Unbekannten gleich dem Range des Coefficientensystems, dann giebt es nur die Lösung $z_1 = 0, \cdots z_q = 0$.

Im Falle $q = r + 1$ ist, kann die Lösung (6) homogener Gleichungen auf bequemere Form gebracht werden. Nehmen wir zu dem Coefficientensysteme noch als erste Zeile hinzu $a_{01}, a_{02}, \cdots a_{0q}$ und bezeichnen wir

$$|a_{\varkappa\lambda}| = \theta \qquad (\varkappa = 0, 1, \cdots r;\ \lambda = 1, 2, \cdots q),$$

dann wird

$$z_1 : z_2 : \cdots : z_q = \frac{\partial\theta}{\partial a_{01}} : \frac{\partial\theta}{\partial a_{02}} : \cdots : \frac{\partial\theta}{\partial a_{0q}}. \tag{6^a}$$

Den Fall $q = r + 2$ kann man auf den vorigen zurückführen, indem man zu den gegebenen homogenen r Gleichungen noch eine mit willkürlichen Coefficienten

$$b_1 z_1 + b_2 z_2 + \cdots + b_q z_q = 0$$

hinzufügt. Dass jede Lösung des erweiterten Systems das gegebene engere auch befriedigt, ist klar. Umgekehrt kann zu jeder Lösung des engeren Systems auf unendlich viele Arten ein passendes System der b bestimmt werden.

Dieser letzte Umstand giebt Veranlassung zu einer interessanten Bemerkung. Wir stellen die linearen, nicht homogenen Gleichungen

$$z_1 = \frac{\partial\theta}{\partial a_{01}}, \ z_2 = \frac{\partial\theta}{\partial a_{02}}, \cdots z_q = \frac{\partial\theta}{\partial a_{0q}}$$

unseres erweiterten Systems auf und betrachten in ihnen die b als Unbekannte. Da dieses System unendlich viele Lösungen besitzt, so muss seine Determinante verschwinden. Dabei erscheint die Determinante als **halbsymmetrische**. Fügen wir dem Systeme der a_{ik} noch zwei ganz beliebige Zeilen oben an

$$b_1, b_2, \cdots b_q \quad \text{und} \quad c_1, c_2, \cdots c_q$$

und nennen die Determinante der b, c, a, welche von der Ordnung $r + 2$ ist, T, so wird jene halbsymmetrische Determinante

$$\begin{vmatrix} 0 & \frac{\partial^2 T}{\partial b_1 \partial c_2} & \frac{\partial^2 T}{\partial b_1 \partial c_3} & \cdots \\ \frac{\partial^2 T}{\partial b_2 \partial c_1} & 0 & \frac{\partial^2 T}{\partial b_2 \partial c_3} & \cdots \\ \frac{\partial^2 T}{\partial b_3 \partial c_1} & \frac{\partial^2 T}{\partial b_3 \partial c_2} & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix} = 0.$$

Bekanntlich ist diese Determinante für gerade r ein Quadrat, dessen zweite Wurzel als **Pfaffian** bezeichnet wird. **Ein Pfaffian** $(r+2)^{\text{ter}}$, **gerader, Ordnung** $|d_{\varkappa\lambda}|$ **verschwindet, wenn seine Elemente**

$$d_{\varkappa\lambda} = \frac{\partial^2 T}{\partial b_\varkappa \partial c_\lambda}$$

gesetzt werden.

§ 481. Aus (6) geht hervor, dass die Gesammtheit der Lösungen von (4^a) $(q - r)$ willkürliche Parameter einschliesst. Die Lösung (6) ist, wie wir gezeigt haben, die allgemeine Lösung. Diese hat aber insofern etwas Unbefriedigendes, als die einzelnen Unbekannten nicht gleichmässig behandelt werden; $z_{r+1}, \cdots z_q$ können ganz willkürlich gewählt werden, während $z_1, \cdots z_r$ dadurch bestimmt sind.

Wir wollen versuchen, diesem Uebelstande dadurch abzuhelfen, dass wir sämmtliche z als lineare homogene Functionen von $(q - r)$ Unbestimmten darstellen, denen jede Werthcombination beigelegt werden darf.

Wählt man $(q - r)$ Systeme

$$(7) \quad z'_{r+1}, z'_{r+2}, \cdots z'_q;\; z''_{r+1}, z''_{r+2}, \cdots z''_q; \cdots;\; z^{(q-r)}_{r+1}, z^{(q-r)}_{r+2}, \cdots z^{(q-r)}_q,$$

so wollen wir diese von einander unabhängig nennen, wenn die Determinante

$$| z^{(\alpha)}_\beta | \qquad (\alpha = 1, 2, \cdots q - r;\; \beta = r + 1,\, r + 2, \cdots q)$$

von Null verschieden ist. Aus solchen $(q - r)$ unabhängigen Systemen kann durch homogene lineare Combination jedes andere System $z^{(0)}_{r+1}, \cdots z^{(0)}_q$ dargestellt werden:

$$(8) \quad \tau_1 z'_{r+\alpha} + \tau_2 z''_{r+\alpha} + \cdots + \tau_{q-r} z^{(q-r)}_{r+\alpha} = z^{(0)}_{r+\alpha} \qquad (\alpha = 1, 2, \cdots q - r).$$

Wir wählen nun $(q - r)$ unabhängige Systeme (7) und bestimmen zu jedem α^{ten} $(\alpha = 1, 2, \cdots q - r)$ durch (6) die Grössen

$$z_1^{(\alpha)},\; z_2^{(\alpha)}, \cdots z_r^{(\alpha)}.$$

Dann liefern die q Werthe von $z_1, \cdots z_q$

$$z^{(\alpha)}_1,\; z^{(\alpha)}_2, \cdots z^{(\alpha)}_r;\; z^{(\alpha)}_{r+1}, \cdots z^{(\alpha)}_q \qquad (\alpha = 1, 2, \cdots q - r)$$

Lösungen von (4^a); und wenn nun

$$z^{(0)}_1,\; z^{(0)}_2, \cdots z^{(0)}_r;\; z^{(0)}_{r+1}, \cdots z^{(0)}_q$$

die aus (6) entspringende, zu den willkürlichen $z^{(0)}_{r+1}, \cdots z^{(0)}_q$ gehörige Lösung von (4^a) darstellt, so folgt wegen (8), dass

$$z_\varrho^{(0)} = \tau_1 z_\varrho' + \tau_2 z_\varrho'' + \cdots + \tau_{q-r} z_\varrho^{(q-r)} \qquad (\varrho = 1, 2, \cdots q)$$

ist, dass man also alle Coordinaten $z_\varrho^{(0)}$ der allgemeinen Lösung in der nämlichen Weise als lineare homogene Functionen von $(q - r)$ Parametern τ darstellen kann.

Achtundvierzigste Vorlesung.

Der Hilbert'sche Irreductibilitäts-Satz.

§ 482. Ist eine ganze, ganzzahlige, irreductible Function der Veränderlichen $x, y, \cdots w$; $q, r, \cdots t$ vorgelegt, und behalten wir in dieser Function einige der Veränderlichen, etwa $x, y, \cdots w$ als Unbestimmte bei, während wir für die übrigen $q, r, \cdots t$ irgend welche ganzen Zahlen einsetzen, so entsteht ein System von unbegrenzt vielen ganzen, ganzzahligen Functionen von $x, y, \cdots w$; es fragt sich, ob in diesem Systeme nothwendig irreductible Functionen der Veränderlichen $x, y, \cdots w$ vorhanden sein müssen. Diese Frage ist für die gesammte Algebra von der grössten Wichtigkeit. Ihre Erledigung hat sie durch eine Arbeit von D. Hilbert, J. f. M. 110 (1892) p. 104 gefunden, in welcher die aufgeworfene Frage bejaht wird. Die Behandlung derselben musste von unseren Untersuchungen über Reductibilität und Irreductibilität (Vorlesung 31) getrennt werden, weil Reihenentwickelungen zu dem Beweise nothwendig sind, die erst an späterer Stelle (Vorlesung 35, § 371) hergeleitet wurden. Wir wollen hier den Hilbert'schen Beweis mit einigen kleinen Aenderungen wiedergeben.

Die Darlegungen beruhen auf dem folgenden Hülfssatze:

Es sei eine unendliche Zahlenreihe $a_1, a_2, a_3, \cdots a_s, \cdots$ vorgelegt, in welcher allgemein a_s eine der a ganzen positiven Zahlen $1, 2, 3, \cdots a$ bedeutet. Es sei überdies m irgend eine ganze positive Zahl. Dann lassen sich stets $(m-1)$ ganze positive Zahlen $\delta_1, \delta_2, \cdots \delta_{m-1}$ bestimmen $(\delta_1 < \delta_2 < \cdots < \delta_{m-1})$, so dass unendlich viele Indices μ bestehen, für welche alle die Zahlen

$$(1) \qquad a_\mu, \; a_{\mu+\delta_1}, \; a_{\mu+\delta_2}, \; \cdots \; a_{\mu+\delta_{m-1}}$$

einen gleichen, von jenen Werthen μ unabhängigen Werth annehmen.

Wir beachten zunächst, dass unter je $(a+1)$ Elementen der vorgelegten Zahlenreihe, die wir als aufeinanderfolgend annehmen und als ein „Intervall“ bezeichnen wollen, mindestens einer der Werthe $1, 2, \cdots a$ wenigstens zweimal auftritt. Ebenso kommt in einem Intervall von der Ausdehnung $(m-1)a+1$ eins der Elemente mindestens m-mal vor. Es mag dies bei einem bestimmten Intervalle das Element a' sein. Die Indices derjenigen m ersten Elemente des Intervalles, welche diesen Werth a' haben, mögen in ansteigender Grösse geordnet die folgenden werden:

$$(1^a) \qquad \mu', \mu'+\delta_1', \; \mu'+\delta_2', \; \cdots \mu'+\delta_{m-1}'.$$

Schiebt man ein Intervall von gleicher Ausdehnung an das erste, so giebt es in diesem neuen gleichfalls ein m-mal vorkommendes Element, etwa a'', welches zu den Indices

$$(1^b) \qquad \mu'', \ \mu''+\delta_1'', \ \mu''+\delta_2'', \ \cdots \mu''+\delta_{m-1}''$$

gehören mag; u. s. f.

Die m Stellen, welche a' in seinem Intervall, a'' in dem seinigen u. s. f. annehmen kann, sind der Zahl nach beschränkt; damit ist es die Wahl der δ_λ. Bei der Ausdehnung $(m-1)a+1$ des Intervalles wird

$$b = \binom{(m-1)a+1}{m}$$

eine obere Grenze für diese Möglichkeiten. Ebenso ist der Werth jedes $a', a'', \cdots$ auf eine der a Möglichkeiten $1, 2, \cdots a$ beschränkt. Also giebt es für die verschiedenen a und δ höchstens $a \cdot b$ Combinationen.

Wählt man also ein Intervall von der Ausdehnung

$$(ab+1)([m-1]a+1),$$

so giebt es in diesem gewiss zwei Indicesreihen (1^a), die in den δ und in dem zugehörigen a übereinstimmen. Ebenso kommen in einem Intervall von der Ausdehnung $(\varkappa ab+1)([m-1]a+1)$ mindestens $(\varkappa+1)$ solche Indicesreihen vor, die in den Werthen der δ und in der Grösse des zugehörigen a übereinstimmen.

Damit ist der Hülfssatz bewiesen.

§ 483. Wir kehren jetzt zu unserem Problem zurück und betrachten eine ganze, ganzzahlige Function von x und t

$$(2) \qquad f(x,t) = Tx^n + T_1x^{n-1} + \cdots + T_n,$$

in welcher $T, T_1, \cdots T_n$ ganze, ganzzahlige Functionen von t bedeuten. Wir nehmen an, dass für jeden ganzzahligen Werth von t die Function $f(x,t)$ in zwei ganze, ganzzahlige Functionen von x zerfällt, und wollen beweisen, dass dann auch bei unbestimmten t die Function $f(x,t)$ nicht irreductibel sein kann.

Für die Substitution $x = \frac{z}{T}$ erhalten wir zunächst die Umformung

$$(2^a) \quad g(z,t) = T^{n-1}f(x,t) = z^n + S_1z^{n-1} + S_2z^{n-2} + \cdots + S_n.$$

Dabei setzen wir fest, dass $|t|$ grösser als der Betrag C_0 jeder Wurzel von $T=0$ angenommen werden soll.

Mit f wird auch g für jedes ganzzahlige t reductibel.

Wir entwickeln nun die n Wurzeln $z_1, z_2, \cdots z_n$ von $g(z,t)=0$ nach fallenden Potenzen von t. Gemäss § 373 können wir $t=\tau^r$ setzen,

wo r so gewählt ist, dass die Entwickelungen aller Wurzeln z_λ nach fallenden ganzen Potenzen von τ vor sich gehen

$$(3)\quad z_\lambda = \alpha_{\lambda 0}\tau^h + \alpha_{\lambda 1}\tau^{h-1} + \cdots + \alpha_{\lambda h} + \frac{\beta_{\lambda 1}}{\tau^1} + \frac{\beta_{\lambda 2}}{\tau^2} + \frac{\beta_{\lambda 3}}{\tau^3} + \cdots \quad (\lambda = 1, 2, \cdots n).$$

Hierbei sind die Coefficienten α und β sämmtlich vollständig bestimmte, rationale oder irrationale, reelle oder imaginäre Zahlen. Die Potenzeihen convergiren stets, wenn $|t|$ eine gewisse positive Grösse C_1 überschreitet. Wir setzen fest, dass $|t|$ oberhalb einer Grenze C, welche grösser als C_0 und C_1 sein soll, angenommen werde.

Nun bilden wir sämmtliche ganzen Functionen von z

$$(4)\qquad \prod_{\varrho=i_1}^{i_m}(z - z_\varrho) \qquad (m = 1, 2, \cdots n - 1),$$

wobei $i_1, i_2, \cdots i_m$ alle möglichen Combinationen der Zahlen $1, 2, \cdots n$ durchlaufen. Die Anzahl der so erhaltenen ganzen Functionen von z beträgt $(2^n - 2)$; wir wollen $2^n - 2 = a$ setzen und die Functionen (4) in beliebiger Reihenfolge mit

$$(4^a)\qquad \varphi_1(z),\ \varphi_2(z),\ \cdots \varphi_a(z) \qquad (a = 2^n - 2)$$

bezeichnen.

Tragen wir die Entwickelungen (3) in alle Functionen (4^a) ein, so erhalten wir für eine jede einen Ausdruck, der in z ganz ist; bei dem der Coefficient der höchsten Potenz gleich 1 wird; und bei dem die Coefficienten der folgenden Potenzen von z Potenzreihen sind, die nach ganzen, fallenden Potenzen von τ fortschreiten. Wir wollen die bei den $\varphi_\varkappa$ auftretenden Potenzreihen mit

$$\mathfrak{P}_\varkappa'(\tau),\ \mathfrak{P}_\varkappa''(\tau),\ \cdots \quad \text{und allgemein mit} \quad \mathfrak{P}_\varkappa(\tau)$$

bezeichnen. Der höchste in irgend einem $\mathfrak{P}$ vorkommende Exponent von τ sei $(m - 1)$.

Nun sei t_0 irgend ein für t erlaubter Werth, und $\tau_0^r = t_0$. Für τ setzen wir jetzt ein $\tau_0, 2\tau_0, 3\tau_0, \cdots \sigma\tau_0, \cdots$ d. h. für t die Werthe $\tau_0^r, 2^r\tau_0^r, 3^r\tau_0^r, \cdots \sigma^r\tau_0^r, \cdots$ Dadurch gehen die $\mathfrak{P}_\varkappa(\tau)$ in Potenzreihen über, die nach ganzen fallenden Potenzen von σ fortschreiten. Wir setzen

$$\mathfrak{P}_\varkappa(\sigma\tau_0) = \overline{\mathfrak{P}}_\varkappa(\sigma)$$

und schreiben die Entwickelung

$$(5)\qquad \overline{\mathfrak{P}}_\varkappa(\sigma) = \sum_{\varrho=1}^{m} A_{\varkappa\varrho}\,\sigma^{m-\varrho} + \sum_{\varrho=1}^{\infty} \frac{B_{\varkappa\varrho}}{\sigma^\varrho} \qquad (\varkappa = 1, 2, \cdots a).$$

Lassen wir nun σ die Zahlenreihe $1, 2, 3, \cdots$ durchlaufen, so muss für jeden dieser Werthe ein Index $\varkappa$ bestehen, für den $\varphi_\varkappa$ eine ganze,

ganzzahlige Function von z wird; denn die Functionen (4^a) liefern alle überhaupt möglichen Factoren von $g(z, t)$. Für diesen Index x müssen also alle zugehörigen Reihen (5) ganzzahlige Werthe haben. Wir setzen fest, dass $x = a_\sigma$ dieser zu σ gehörige Index sei, der dann einen der Werthe $1, 2, \cdots a$ hat.

§ 484. Wir stehen jetzt auf dem Boden des Hülfssatzes § 482 und können daher $(m - 1)$ feste Indices $\delta_1, \delta_2, \cdots \delta_{m-1}$ so bestimmen, dass es unendlich viele Zahlen μ giebt, für welche alle

$$a_\mu, \; a_{\mu+\delta_1}, \; a_{\mu+\delta_2}, \; \cdots a_{\mu+\delta_{m-1}}$$

den gleichen Werth haben. Setzen wir diesen gleich α, so werden für die unendlich vielen μ sämmtliche Potenzreihen

$$\overline{\mathfrak{P}}_\alpha(\mu), \; \overline{\mathfrak{P}}_\alpha(\mu + \delta_1), \; \overline{\mathfrak{P}}_\alpha(\mu + \delta_2), \; \cdots \overline{\mathfrak{P}}_\alpha(\mu + \delta_{m-1})$$

ganze Zahlen liefern.

Zur Abkürzung setzen wir jetzt den Complex der Glieder aus $\overline{\mathfrak{P}}_\alpha(\mu)$, die keine negativen Potenzen von μ enthalten, gleich $p_\alpha(\mu)$ und seine Ableitungen nach μ gleich $p_\alpha'(\mu), p_\alpha''(\mu), \cdots$. Dann wird

$$\begin{aligned}\overline{\mathfrak{P}}_\alpha(\mu + \delta) = p_\alpha(\mu) + p_\alpha'(\mu)\cdot\frac{\delta}{1} + p_\alpha''(\mu)\cdot\frac{\delta^2}{1\cdot 2} + \cdots + p_\alpha^{(m-1)}(\mu)\cdot\frac{\delta^{m-1}}{(m-1)!} \\ (6) \qquad + \sum_{\varrho=1}^{\infty}\left(B_{\alpha\varrho}\sum_{\lambda=0}^{\infty}\frac{c_{\varrho\lambda}\delta^\lambda}{\mu^{\varrho+\lambda}}\right);\end{aligned}$$

hierin bedeuten die $c_{\varrho\lambda}$ die bei der Entwickelung von

$$\frac{1}{(1+\delta)^\varrho} = 1 - \binom{\varrho}{1}\delta + \binom{\varrho+1}{2}\delta^2 - \binom{\varrho+2}{3}\delta^3 + \cdots$$

auftretenden Coefficienten.

Wir suchen nun die m Unbekannten $u_0, u_1, u_2, \cdots u_{m-1}$ ganzzahlig so zu bestimmen, dass in dem Aggregate

$$(7) \quad - u_0\overline{\mathfrak{P}}_\alpha(\mu) + u_1\overline{\mathfrak{P}}_\alpha(\mu + \delta_1) + \cdots + u_{m-1}\overline{\mathfrak{P}}_\alpha(\mu + \delta_{m-1}) = P(\mu)$$

keine ganzen positiven Potenzen von μ vorkommen. Dazu reicht es aus, die u so zu wählen, dass das System linearer Gleichungen

$$\begin{aligned} u_1 + \quad u_2 + \cdots + \quad u_{m-1} &= u_0, \\ \delta_1 u_1 + \quad \delta_2 u_2 + \cdots + \delta_{m-1}u_{m-1} &= 0, \\ \delta_1^2 u_1 + \quad \delta_2^2 u_2 + \cdots + \delta_{m-1}^2 u_{m-1} &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \delta_1^{m-1}u_1 + \delta_2^{m-1}u_2 + \cdots + \delta_{m-1}^{m-1}u_{m-1} &= 0 \end{aligned}$$

ganzzahlig erfüllt werde, was stets möglich ist, sobald man u_0 als ganzes Vielfaches der nicht verschwindenden Determinante

$$\left|\delta_\alpha^{\beta-1}\right| \qquad (\alpha, \beta = 1, 2, \cdots m)$$

annimmt. Aus der Structur der inneren Summe auf der rechten Seite von (6) erkennt man, dass bei jedem $B_{\alpha\varrho}$ die ersten m Glieder, d. h. diejenigen mit $\lambda = 0, 1, \cdots (m-1)$ wegfallen. Das nächste Glied dagegen, dasjenige mit $\lambda = m$, kann nicht verschwinden, weil die Gleichung

$$\delta_1^m u_1 + \delta_2^m u_2 + \cdots + \delta_{m-1}^m u_{m-1} = 0$$

in Verbindung mit dem obigen linearen Systeme fordern würde, dass

$$|\delta_\alpha^\beta| = 0 \qquad (\alpha, \beta = 1, 2, \cdots m)$$

erfüllt wäre, was ja nicht der Fall ist.

Ist deshalb in (6) $B_{\alpha v}$ der erste nicht verschwindende Coefficient eines Gliedes mit negativem Exponenten von μ, so beginnt die Entwickelung von (6) nach fallenden Potenzen von μ mit

$$\Gamma_{\alpha v} = B_{\alpha v} \frac{c_{vm}}{\mu^{v+m}} [\delta_1^m u_1 + \delta_2^m u_2 + \cdots + \delta_{m-1}^m u_{m-1}] \neq 0,$$

d. h. der Ausdruck, in den (7) übergeht,

(7a) $P(\mu) = \Gamma_{\alpha v} \cdot \mu^{-v-m} + \Gamma' \cdot \mu^{-v-m-1} + \cdots \qquad (\Gamma_{\alpha v} \neq 0)$

wird für unendlich viele Werthe von μ rational und ganz. Lässt man aber μ hinlänglich gross werden, so wird der Werth von (7a) kleiner als 1 und folglich gleich 0; d. h. (7a) verschwindet für unendlich viele μ. Andererseits erkennt man aus der Form

$$P(\mu) = \mu^{-v-m} [\Gamma_{\alpha v} + \Gamma' \mu^{-1} + \cdots],$$

dass dies nicht möglich ist, da für hinlänglich grosse μ der Werth von $P(\mu)$ beliebig nahe an $\Gamma_{\alpha v} \cdot \mu^{-v-m}$ gebracht werden kann.

Aus diesem Widerspruche schliessen wir, dass in (6) überhaupt kein von Null verschiedenes B existirt. Wir haben daher: Die Function

(5a) $$\mathfrak{P}_\alpha(\sigma) = \sum_{\varrho=1}^{m} A_{\alpha\varrho} \sigma^{m-\varrho}$$

besitzt für unendlich viele ganzzahlige Werthe σ selbst ganzzahlige Werthe. Daraus schliessen wir, dass die A sämmtlich rationale Grössen sind. Denn schreibt man die Gleichung (5a) für m solche Werthe $\sigma = \mu_1, \mu_2, \cdots \mu_m$ an und berechnet daraus bei festem α die A, dann erhält man rationale Lösungen der linearen Gleichungen.

Geht man von (5a) auf die $\mathfrak{P}(\tau)$ zurück, so folgt

(8) $$\mathfrak{P}_\alpha(\tau) = A_{\alpha 1} \left(\frac{\tau}{\tau_0}\right)^{m-1} + A_{\alpha 2} \left(\frac{\tau}{\tau_0}\right)^{m-2} + \cdots + A_{\alpha m},$$

wobei die A rationale Grössen sind.

Durch (8) hat sich dem τ_0 ein Index α zugeordnet, der a nicht überschreitet. Wählen wir jetzt $\tau_0, \tau_1, \tau_2, \cdots \tau_a$ innerhalb des erlaubten Gebietes für t, nehmen wir die τ ferner von einander verschieden und

als Primzahlen an, dann müssen mindestens zwei τ vorhanden sein, die dasselbe α haben. Es seien dies etwa τ_0 und τ_1; dann hat man

$$\mathfrak{P}_\alpha(\tau) = \mathfrak{A}_{\alpha 1}\left(\frac{\tau}{\tau_1}\right)^{m-1} + \mathfrak{A}_{\alpha 2}\left(\frac{\tau}{\tau_1}\right)^{m-2} + \cdots + \mathfrak{A}_{\alpha m},$$

worin auch die $\mathfrak{A}$ rationale Grössen sind.

Vergleicht man die beiden letzten Ausdrücke und geht von τ_0, τ_1 auf t_0, t_1 zurück, so folgt

$$\mathfrak{A}_{\alpha 1} t_0^{\frac{m-1}{r}} = A_{\alpha 1} t_1^{\frac{m-1}{r}}, \quad \mathfrak{A}_{\alpha 2} t_0^{\frac{m-2}{r}} = A_{\alpha 2} t_1^{\frac{m-2}{r}}, \cdots;$$

und da die t_0, t_1 von einander verschiedene Primzahlen und die $\mathfrak{A}$, A rationale Zahlen sind, so ist dies nur möglich, wenn die Coefficienten in allen den Relationen Null werden, bei denen der Exponent der t keine ganze Zahl ist. Folglich kommen in $\mathfrak{P}_\alpha(\tau)$ nur ganze Potenzen von τ^r, d. h. von t vor.

Man hat daher unter den Functionen (4^a) für ein gewisses α

$$\varphi_\alpha(z) = \Psi(z, t),$$

wo Ψ eine ganze Function von z und von t mit rationalen Zahlencoefficienten bedeutet; (2^a) wird $g(z, t) = \Psi(z, t) \cdot \Psi_1(z, t)$, und

$$f(x, t) = \frac{\Psi(x, t) \cdot \Psi_1(x, t)}{T^{n-1}}$$

oder, wenn man von den rationalen zu ganzzahligen Coefficienten übergeht,

$$= \frac{\Phi(x, t) \cdot \Phi_1(x, t)}{A \cdot T^{n-1}}.$$

Hierin sind f, Φ, Φ_1 ganze, ganzzahlige Functionen von x und t, ferner ist T eine ganze, ganzzahlige Function von t und A eine ganze Zahl. Nach § 343 muss dann auch eine Zerlegung

$$f(x, t) = \varphi(x, t) \cdot \varphi_1(x, t)$$

bestehen, wenn wir jetzt unter φ und φ_1 ganze, ganzzahlige Functionen verstehen.

Damit ist der behauptete Satz bewiesen. Wir können ihn so aussprechen, dass wir sagen: W e n n $f(x, t)$ f ü r a l l e g a n z z a h l i g e n W e r t h e v o n t, d i e o b e r h a l b e i n e r g e w i s s e n G r e n z e C l i e g e n, i n F a c t o r e n z e r f ä l l t, d a n n i s t e s r e d u c t i b e l. Folglich giebt es oberhalb einer Grenze C einen Werth von t, für den eine irreductible Function $f(x, t)$ von x und von t irreductibel bleibt. Ist t' dieser Werth, nimmt man eine weitere Grenze $C' > t_0$ an, so folgt die Existenz eines zweiten Werthes t'', für den f irreductibel bleibt u. s. f. Es g i e b t u n e n d l i c h v i e l e C o n s t a n t e n $t^{(\lambda)}$, f ü r w e l c h e $f(x, t^{(\lambda)})$ i r r e d u c t i b e l b l e i b t, f a l l s $f(x, t)$ i n x u n d t i r r e d u c t i b e l i s t.

§ 485. Wenn $f(x, t)$, $g(x, t)$, $\cdots k(x, t)$ sämmtlich ganze, ganzzahlige, irreductible Functionen der beiden Veränderlichen x und t sind, so ist es stets auf unendlich viele Weisen möglich, für t eine ganze rationale Zahl einzusetzen, so dass dadurch jede dieser Functionen $f(x, t)$, $g(x, t)$, $\cdots k(x, t)$ in eine irreductible Function der einen Veränderlichen x übergeht.

Um dies zu beweisen, stellen wir die Wurzeln aller der Gleichungen

$$f(x, t) = 0, \quad g(x, t) = 0, \quad \cdots \quad k(x, t) = 0$$

dar, wie dies in (3) bei einer Gleichung geschehen ist, bilden dann die Functionen, welche denen in (4^a) entsprechen,

$$\varphi_\alpha(z), \quad \gamma_\alpha(z), \quad \cdots \quad \varkappa_\alpha(z),$$

betrachten weiter die Systeme aller hierzu gehörigen Coefficienten-Potenzreihen, und verfahren genau so, wie dies oben geschehen ist. Dann zeigt es sich: wenn für jeden Werth des t mindestens eine der Functionen zerfällt, muss mindestens eine unter ihnen reductibel sein.

Sprechen wir den Satz für das Product $F(x, t)$ der sämmtlichen vorgelegten Functionen $f(x, t)$, $g(x, t)$, $\cdots k(x, t)$ aus, so ergiebt sich folgendes Theorem:

In einer beliebig gegebenen ganzen, ganzzahligen Function $F(x, t)$ der beiden Veränderlichen x und t lässt sich stets für t auf unendlich viele Weisen eine ganze Zahl derart einsetzen, dass in Bezug auf die Veränderliche x die entstehende Function genau in ebensoviele ganze, ganzzahlige, irreductible Functionen zerfällt, wie die ursprüngliche Function $F(x, t)$ bei unbestimmtem Parameter t. (Hilbert, l. c. S. 117.)

§ 486. Zum Zwecke der weiteren Ausdehnung des Theorems aus § 484 brauchen wir zunächst aus der Theorie der Functionen folgenden Satz. Es sei die Gleichung $\psi(z;\ t, r, \cdots q) = 0$ mit der Unbekannten z und den Parametern $t, r, \cdots q$ vorgelegt; es mögen $t_0, r_0, \cdots q_0$ Werthe des Parameters sein, für die $\psi(z;\ t_0, r_0, \cdots q_0) = 0$ lauter verschiedene Wurzeln besitzt. Dann lassen sich alle Wurzeln $z_1, z_2, \cdots z_n$, welche $\psi(z;\ t, r, \cdots q) = 0$ hat, in der Form von Potenzreihen

$$(9) \qquad z_\alpha = \sum c^{(\alpha)}_{\varkappa, \lambda, \cdots \nu} (t - t_0)^\varkappa (r - r_0)^\lambda \cdots (q - q_0)^\nu \quad (\alpha = 1, 2, \cdots n)$$

darstellen, welche nach positiven, steigenden Potenzen von

$$(t - t_0), \ (r - r_0), \ \cdots (q - q_0)$$

fortschreiten und für hinlänglich kleine absolute Beträge dieser Differenzen convergiren. —

Wir wollen nun beweisen, dass wenn $F(x;\ t, r, \cdots q)$ eine irreductible ganze, ganzzahlige Function der Veränderlichen x und der

Parameter $t, r, \cdots q$ bezeichnet, stets für $t, r, \cdots q$ lineare, ganze, ganzzahlige Functionen eines Parameters u eingesetzt werden können, so dass dadurch die Function in eine irreductible Function der beiden Veränderlichen x und u übergeht.

Es sei

$$F(x;\ t, r, \cdots q) = f x^n + f_1 x^{n-1} + \cdots + f_n,$$

wo $f, f_1, \cdots f_n$ ganze ganzzahlige Functionen von $t, r, \cdots q$ sind. Setzen wir hierin $x = \frac{z}{f}$ ein und multipliciren dann mit f^{n-1}, so ergiebt sich eine gleichfalls irreductible Function

$$G(z;\ t, r, \cdots q) = z^n + g_1 z^{n-1} + \cdots + g_n,$$

wo $g_1, g_2, \cdots g_n$ wiederum ganze Functionen von $t, r, \cdots q$ sind. Wir bilden die Discriminante $D(t, r, \cdots q)$ von G; diese ist nicht identisch Null, weil sonst G einen quadratischen Factor besässe. Es möge $t_0, r_0, \cdots q_0$ ein System ganzer Zahlen bedeuten, für welches D nicht verschwindet. Dann gelten für alle Wurzeln $z_1, z_2, \cdots z_n$ von $G = 0$ Entwickelungen von der Form (9). Eine Beschränkung der Bestimmung von $t_0, r_0, \cdots q_0$ wird noch eintreten (S. 202, Z. 10); diese ändert aber an unseren Ueberlegungen nichts.

Jetzt bilden wir genau wie im früheren Falle alle Functionen

$$\prod_{q=i_1}^{i_m} (z - z_q) \qquad (m = 1, 2, \cdots n-1) \tag{4}$$

und setzen in diese ganzen Functionen von z die Entwickelungen der Wurzeln z_q von der Form (9) ein. Dann kann in keiner der erhaltenen Functionen die Gesammtheit der als Coefficienten auftretenden Potenzreihen im Endlichen abbrechen; denn sonst hätte $G(z;\ t, r, \cdots q)$ gerade diese Function als ganzen Theiler in z mit rationalen Coefficienten in den Parametern. Das würde aber die Voraussetzung der Irreductibilität verletzen.

Nun setzen wir in diese so entwickelten Functionen (4) ein

$$t = t_1 u + t_0, \quad r = r_1 u + r_0, \quad \cdots q = q_1 u + q_0, \tag{10}$$

wobei $t_1, r_1, \cdots q_1$ noch unbestimmte ganze Zahlen und u eine Variable sein sollen; es ist dann unsere Aufgabe zu zeigen, dass man stets für $t_1, r_1, \cdots q_1$ ganze rationale Zahlen derart wählen kann, dass auch nach dieser Substitution nicht alle Potenzreihen irgend einer Function (4) im Endlichen abbrechen. Das allgemeine Glied der entwickelten Function (4) enthält Coefficienten der Potenzen von z von der Form

$$C_{\varkappa, \lambda, \cdots \nu}(t - t_0)^{\varkappa}(r - r_0)^{\lambda} \cdots (q - q_0)^{\nu};$$

diese gehen jetzt in

$$C_{\varkappa,\lambda,\cdots\nu} t_1^\varkappa r_1^\lambda \cdots q_1^\nu \cdot u^{\varkappa+\lambda+\cdots+\nu}$$

über. Ordnen wir nach Potenzen von u, so entsteht die Reihe

$$\sum_{m=0}^{\infty} u^m \sum C_{\varkappa,\lambda,\cdots\nu} t_1^\varkappa r_1^\lambda \cdots q_1^\nu \quad (\varkappa+\lambda+\cdots+\nu=m).$$

Falls eine der ursprünglichen Reihen in $(t-t_0), (r-r_0), \cdots (q-q_0)$ im Endlichen nicht abbricht, liefert die transformirte Reihe beliebig hohe Potenzen u^m von u, deren Coefficienten nicht identisch verschwindende ganze Functionen von $t_1, r_1, \cdots q_1$ sind. Daher zeigen die in § 337 angestellten Schlüsse, dass $t_1, r_1, \cdots q_1$ ganzzahlig so gewählt werden können, dass der Coefficient von u^m nicht verschwindet.

Demnach brechen nicht sämmtliche zu einer Function (4) gehörigen Reihen nach Substitution (10) im Endlichen ab. Denn sonst würde (10) aus $G(z; t, r, \cdots q)$ eine zerfallende Function von z und u herleiten; wäre nun in ihr d die Summe der höchsten vorkommenden Exponenten bei $t, r, \cdots q$, so könnte in den Reihen (11) kein u^m mit $m > d$ vorkommen, dessen Coefficient von Null verschieden ist. Wir haben aber bei beliebig hoch angenommener Zahl m gleichwohl den Coefficienten von u^m von Null verschieden machen können. Also kann man in (10) die Werthe $t_1, r_1, \cdots q_1$ ganzzahlig derart wählen, dass $G(z; t, r, \cdots q)$ irreductibel bleibt.

Wenn wir also in der ursprünglich vorgelegten Function $F(x; t, r, \cdots q)$ die Substitution (10) ausführen, so folgt, dass die entstehende Function der beiden Veränderlichen x, u keinesfalls in mehrere von x abhängige Factoren zerfällt. Es bliebe mithin für eine Zerfällung nur die Möglichkeit, dass die aus $F(x; t, r, \cdots q)$ vermöge (10) entstehende Function einen Factor besitzt, der allein die Veränderliche u enthält. Nun war

$$F(x; t, r, \cdots q) = f(t, r, \cdots q) \cdot x^n + f_1(t, r, \cdots q) \cdot x^{n-1} + \cdots,$$

wobei die Coefficienten $f, f_1, \cdots$ keinen gemeinsamen Factor in $t, r, \cdots q$ besitzen. Wir tragen $t = t' + t_0$, $r = r' + r_0$, $\cdots$ $q = q' + q_0$ ein und erhalten

$$F(x; t, r, \cdots q) = h(t', r', \cdots q') \cdot x^n + h_1(t', r', \cdots q') \cdot x^{n-1} + \cdots,$$

wobei auch $h, h_1, \cdots$ keinen gemeinsamen Factor in $t', r', \cdots q'$ haben. Man kann deshalb nach § 346, XII ganze, ganzzahlige Functionen $\varphi, \varphi_1, \cdots$ von $t', r', \cdots q'$ bestimmen, so dass

$$h(t', r', \cdots q') \cdot \varphi(t', r', \cdots q') + h_1(t', r', \cdots) \cdot \varphi_1(t' r', \cdots) + \cdots = \Phi(r', \cdots q')$$

von t' frei wird. Macht man nun $t' = t_1 u$, $r' = r_1 u$, $\cdots$ $q' = q_1 u$, dann erhält man die Substitution (10), und es folgt, dass, wenn

$$h(t_1 u, r_1 u, \cdots q_1 u), \quad h_1(t_1 u, r_1 u, \cdots q_1 u), \cdots$$

als gemeinsamen Theiler eine Function von u hätten, diese von t_1 unabhängig sein müsste. Aus dem gleichen Grunde könnte dieser Theiler auch nicht von $r_1, \cdots q_1$ abhängen; also müsste er eine Function von u allein sein. Ordnet man jedoch die $h_\alpha(t_1 u, r_1 u, \cdots q_1 u)$ nach Potenzproducten der $t_1, r_1, \cdots q_1$, so sieht man, dass jener Theiler in u alle Coefficienten der Potenzproducte theilen müsste. Diese Coefficienten sind von constanten Factoren abgesehen lediglich Potenzen von u; folglich kann der Factor der h_α oder der f_α in F nur von der Form u^x sein. Dass dies in der That möglich ist, sieht man sofort ein. Man kann dieser Möglichkeit aber ausweichen, wenn man $t_0, r_0, \cdots q_0$ so bestimmt, dass mindestens eine der Functionen $h, h_1, \cdots$ ein von $t', r', \cdots q'$ unabhängiges nicht verschwindendes Glied besitzt, weil dann der Factor u^x in u^0 übergehen muss. Ist eine solche Bestimmung getroffen, dann kann man $t_1, r_1, \cdots q_1$ den obigen Vorschriften gemäss wählen, ohne dass F zerfällt. Hiermit ist der Hülfssatz vollständig bewiesen.

§ 487. Wir kommen nunmehr zu dem Beweise des Hauptsatzes: Wenn $F(x, y, \cdots w;\ t, r, \cdots q)$ eine irreductible, ganze, ganzzahlige Function der Veränderlichen $x, y, \cdots w$ und der Parameter $t, r, \cdots q$ bezeichnet, so ist es stets auf unendlich viele Weisen möglich, für die Parameter $t, r, \cdots q$ ganze rationale Zahlen einzusetzen, so dass dadurch die Function $F(x, y, \cdots w;\ t, r, \cdots q)$ in eine irreductible Function der Veränderlichen $x, y, \cdots w$ übergeht. (Hilbert l. c. p. 121.)

Wenn wir in der vorgelegten Function $F(x, y, \cdots w;\ t, r, \cdots q)$ zuerst die Substitution

$$y = \eta x, \quad \cdots\cdots \quad w = \omega x$$

vornehmen und dann die etwa als gemeinsamer Factor auftretende Potenz von x fortlassen, so entsteht eine Function $G(x; \eta, \cdots \omega, t, r \cdots q)$ der Veränderlichen x und der Parameter $\eta, \cdots \omega; t, r, \cdots q$, welche ebenfalls irreductibel ist. Wir setzen, was nach dem eben bewiesenen Satze möglich ist, für diese Parameter lineare ganzzahlige Functionen eines einzigen Parameters u ein, nämlich

$$\eta = \eta_1 u + \eta_0, \quad \cdots\cdots \quad \omega = \omega_1 u + \omega_0,$$
$$t = t_1 u + t_0, \quad \cdots\cdots \quad q = q_1 u + q_0,$$

so dass jene Function in eine irreductible Function $g(x, u)$ der beiden Veränderlichen x und u übergeht. Es lässt sich dann nach dem Theoreme aus § 484 für u eine ganze rationale Zahl u_0 einsetzen, so dass die Function $g(x, u_0)$ eine irreductible Function der einen Veränderlichen x wird. Nunmehr erkennen wir, dass die ursprünglich

vorgelegte Function $F(x, y, \cdots w;\ t, r, \cdots q)$ nothwendig in eine irreductible Function der Veränderlichen $x, y, \cdots w$ übergeht, wenn wir für die Parameter die ganzen Zahlen

$$t = t_1 u_0 + t_0,\quad r = r_1 u_0 + r_0,\quad \cdots q = q_1 u_0 + q_0$$

einsetzen; denn die so entstehende Function würde in eine irreductible Function der einen Veränderlichen x übergehen, wenn wir überdies noch setzten

$$y = (\eta_1 u_0 + \eta_0)\, x,\quad \cdots\cdot w = (\omega_1 u_0 + \omega_0)\, x$$

und von einer etwa als Factor auftretenden Potenz der Veränderlichen x absehen. Damit ist der verlangte Nachweis geführt.

Neunundvierzigste Vorlesung.

Die cyklischen Gleichungen.

§ 488. Die algebraische Auflösbarkeit der Kreistheilungsgleichungen beruht auf folgendem Umstande: man kann die Gleichungswurzeln in eine solche geschlossene, cyklische Folge bringen, dass eine jede Wurzel dieselbe Function der vorhergehenden wird, wie die zweite von der ersten.

Dass bei den Kreistheilungsgleichungen diese Function gerade in der einfachen Gestalt einer Potenz mit ganzzahligem Exponenten auftrat

$$\omega_2 = \omega_1^g,\quad \omega_3 = \omega_2^g,\quad \cdots\ \omega_{p-1} = \omega_{p-2}^g,\quad \omega_1 = \omega_{p-1}^g,$$

vgl. § 314, (11) Bd. I, ist völlig indifferent, und daher kommt es, dass die bei jenen Gleichungen benutzte Methode sich bei allen cyklischen Gleichungen verwenden lässt, d. h. bei allen solchen, bei denen die Wurzeln in der oben bezeichneten Weise angeordnet werden können*). Bevor wir aber auf diese Art von Gleichungen näher eingehen, wollen wir eine allgemeinere Art von algebraischen Gleichungen besprechen, durch die wir dann naturgemäss auf den besonderen Fall cyklischer Gleichungen geleitet werden. Wir folgen dabei dem Gange von Abel**), von dem diese Untersuchungen stammen.

§ 489. Es sei

$$f(z) \equiv (z - z_1)(z - z_2) \cdots\cdot (z - z_m) = 0 \tag{1}$$

---

*) Kronecker hat diese Gleichungen in seinem Aufsatze: Berl. Ber. 1853, 10. Juni als „Abel'sche Gleichungen" und später ibid. 1878, 16. April als „einfache Abel'sche Gleichungen" bezeichnet.

**) Oeuvres, éd. Sylow et Lie, 1. p. 479.

eine vorgelegte irreductible Gleichung, bei welcher zwei Wurzeln durch eine beliebige rationale Beziehung gemäss der Gleichung

$$z_2 = \varphi(z_1) \tag{2}$$

miteinander verbunden sind; die rationale Function φ können wir ohne Beschränkung als eine ganze Function voraussetzen (§ 108, Bd. I); ihre Coefficienten gehören einem bestimmten Rationalitätsbereiche an, der natürlich auch die Coefficienten von (1) enthält.

Nun hat die Gleichung $f(\varphi(z)) = 0$ mit der irreductiblen Gleichung (1) eine und daher alle Wurzeln gemeinsam; insbesondere ist somit $f(\varphi(z_2)) = 0$, d. h. auch die Grösse $\varphi(z_2) = \varphi(\varphi(z_1)) = \varphi_2(z_1)$ (vgl. § 270, Bd. I) ist eine Wurzel von $f(z) = 0$. In derselben Weise zeigt man, dass alle Glieder der beliebig weit fortgesetzten Reihe von Iterationen

$$z_1, \ \varphi(z_1), \ \varphi_2(z_1), \ \cdots \ \varphi_\lambda(z_1), \ \cdots \ \varphi_{\varkappa+\lambda}(z_1), \ \cdots$$

Wurzeln von (1) liefern.

Da die Anzahl dieser Glieder aber beliebig gross gemacht werden kann, so muss es Indices $\varkappa, \lambda$ geben, für welche

$$\varphi_{\varkappa+\lambda}(z_1) = \varphi_\lambda(z_1) \quad \text{d. h.} \quad \varphi_\varkappa[\varphi_\lambda(z_1)] - [\varphi_\lambda(z_1)] = 0$$

ist. Es haben demnach die beiden Gleichungen

$$\varphi_\varkappa(z) - z = 0, \quad f(z) = 0$$

die Wurzel $\varphi_\lambda(z_1)$ gemeinsam, und wegen der Irreductibilität von $f(z)$ ist daher auch z_1 eine Wurzel der ersten Gleichung; d. h. es giebt einen Index $\varkappa$, für den $\varphi_\varkappa(z_1) = z_1$ wird. Giebt es mehrere solche $\varkappa$ von gleicher Eigenschaft, so sei n der kleinste Werth unter ihnen. Dann sind die Glieder der Reihe

$$z_1, \ \varphi(z_1), \ \varphi_2(z_1), \ \cdots \ \varphi_{n-1}(z_1); \qquad (\varphi_n(z_1) = z_1) \tag{3}$$

sämmtlich von einander verschieden, weil im entgegengesetzten Falle der oben durchgeführte Schluss auf einen noch kleineren Index als n von derselben Eigenschaft leiten würde. Man erkennt ferner, dass

$$\varphi_{n+\alpha}(z_1) = \varphi_\alpha(z_1)$$

für jedes α werden wird, und dass $\varphi_n(z_1), \ \varphi_{2n}(z_1), \ \varphi_{3n}(z_1), \cdots$ die einzigen Iterationen von $\varphi(z_1)$ mit dem Werthe z_1 sind.

Ist die Reihe der Wurzeln von (1) durch die Grössen (3) noch nicht erschöpft, so giebt es eine weitere, nicht in (3) enthaltene Wurzel, die wir z_1' nennen wollen. Da $f(\varphi(z)) = 0$ alle Wurzeln von $f(z) = 0$ enthält, so ist auch $f(\varphi(z_1')) = 0$, und es ist $\varphi(z_1')$ eine Wurzel von (1). Wir wollen sie mit z_2' bezeichnen und setzen also

$$z_2' = \varphi(z_1'). \tag{2a}$$

Hieran knüpfen sich wieder unsere obigen Betrachtungen, und wir ge-

langen auf dem beschrittenen Wege zu einer Reihe von Wurzeln, die sich durch Iteration ergeben,

$$z_1', \ \varphi(z_1'), \ \varphi_2(z_1'), \ \cdots \ \varphi_{\nu-1}(z_1'); \qquad (\varphi_\nu(z_1') = z_1'),$$

wobei ν die kleinste positive, ganze Zahl von der Eigenschaft ist, dass $\varphi_\nu(z_1') = z_1'$ wird. Weil $\varphi_n(z) - z = 0$ und $\varphi_\nu(z) - z = 0$ mit der irreductiblen Gleichung (1) je eine Wurzel gemeinsam haben, nämlich z_1 und bezw. z_1', so besitzt jede der beiden Gleichungen alle Wurzeln von (1), und insbesondere wird $\varphi_n(z_1') = z_1'$ und $\varphi_\nu(z_1) = z_1$. Daraus folgt aber erstens, dass n ein Vielfaches von ν, und zweitens, dass ν ein Vielfaches von n ist, d. h. es wird $n = \nu$, und wir haben deshalb die auf z_1' aufgebaute Wurzelreihe

$$(3^a) \qquad z_1', \ \varphi(z_1'), \ \varphi_2(z_1'), \ \cdots \ \varphi_{n-1}(z_1'); \qquad (\varphi_n(z_1') = z_1').$$

Dabei hat die Wurzelreihe (3^a) mit der Reihe (3) kein Glied gemeinsam. Aus der Gleichheit

$$\varphi_\varrho(z_1') = \varphi_\sigma(z_1)$$

würde nämlich folgen, wenn man auf beiden Seiten mit $\varphi_{n-\varrho}$ iterirt,

$$z_1' = \varphi_{n-\varrho}(\varphi_\varrho(z_1')) = \varphi_{n+\sigma-\varrho}(z_1),$$

so dass gegen die Annahme z_1' in (3) vorkäme.

Ist die Reihe der Wurzeln von (1) durch die beiden Serien (3) und (3^a) noch nicht erschöpft, so gehen wir nach demselben Schema weiter und erkennen damit, dass sich alle Wurzeln $z_1, z_2, \cdots z_m$ in eine Tabelle

$$(4) \qquad \begin{matrix} z_1, & \varphi(z_1), & \varphi_2(z_1), & \cdots \varphi_{n-1}(z_1), \\ z_1', & \varphi(z_1'), & \varphi_2(z_1'), & \cdots \varphi_{n-1}(z_1'), \\ \cdot & \cdot & \cdot & \cdot \\ z_1^{(\nu-1)}, & \varphi(z_1^{(\nu-1)}), & \varphi_2(z_1^{(\nu-1)}), & \cdots \varphi_{n-1}(z_1^{(\nu-1)}) \end{matrix} \qquad (n \cdot \nu = m)$$

einordnen lassen, und dass n ein Theiler von m wird.

Ist $\nu = 1$, so erhält man (1) als cyklische Gleichung. Wir werden zunächst $\nu > 1$ annehmen.

§ 490. Wir wollen unter $S(t_1, t_2, \cdots t_n)$ eine beliebige symmetrische, ganze Function der Argumente $t_1, t_2, \cdots t_n$ verstehen; dann betrachten wir die ν Werthe

$$\begin{aligned} y_1 &= S(z_1, \varphi(z_1), \varphi_2(z_1), \cdots \varphi_{n-1}(z_1)) = F(z_1) = F(\varphi(z_1)) = \cdots \\ y_2 &= S(z_1', \varphi(z_1'), \varphi_2(z_1'), \cdots \varphi_{n-1}(z_1')) = F(z_1') = F(\varphi(z_1')) = \cdots \\ &\cdots\cdots\cdots \\ y_\nu &= S(z_1^{(\nu-1)}, \varphi(z_1^{(\nu-1)}), \cdots \varphi_{n-1}(z_1^{(\nu-1)})) = F(z_1^{(\nu-1)}) = F(\varphi(z_1^{(\nu-1)})) = \cdots \end{aligned}$$

Wir können es durch passende Wahl von S stets so einrichten, und zwar auf beliebig viele Arten, dass alle diese Werthe $y_1, y_2, \cdots y_\nu$

von einander verschieden sind. Dazu reicht es z. B. schon aus, bei unbestimmtem u die Function in der Form

$$y_{\alpha+1} = (u - z^{(\alpha)})\,(u - \varphi(z^{(\alpha)}))\,\cdots\,(u - \varphi_{n-1}(z^{(\alpha)}))$$

anzusetzen, weil nur dann ein Werth $y_{\alpha+1}$ einem anderen $y_{\beta+1}$ gleich werden kann, wenn sämmtliche Wurzeln $z^{(\alpha)}, \cdots$ mit den Wurzeln $z^{(\beta)}, \cdots$ abgesehen von der Reihenfolge übereinstimmen; dies trifft aber nur für $\alpha = \beta$ zu.

Nun wird die Summe der $\varkappa^{\text{ten}}$ Potenzen unserer ν Grössen y

$$\begin{aligned} y_1^\varkappa + y_2^\varkappa + \cdots + y_\nu^\varkappa &= \frac{1}{n}\,(F^\varkappa(z_1) + F^\varkappa(\varphi(z_1)) + \cdots + F^\varkappa(\varphi_{n-1}(z_1))) \\ &\quad + \frac{1}{n}\,(F^\varkappa(z_1') + F^\varkappa(\varphi(z_1')) + \cdots + F^\varkappa(\varphi_{n-1}(z_1'))) \\ &\quad + \cdots\cdots\cdots\cdots \\ &= \frac{1}{n}\,[F^\varkappa(z_1) + F^\varkappa(z_2) \quad + \cdots + F^\varkappa(z_m)] \end{aligned}$$

eine symmetrische Function der Wurzeln von (1) und daher rational in unserem Rationalitätsbereiche darstellbar. Setzen wir $\varkappa = 1, 2, \cdots \nu$ und berechnen daraus nach § 94, Bd. I die elementaren symmetrischen Functionen der $y_1, y_2, \cdots y_\nu$, so erkennen wir, dass die Grössen $y_1, y_2, \cdots y_\nu$ die Wurzeln einer Gleichung ν^{ten} Grades

$$(5) \qquad g(y) \equiv y^\nu - d_1 y^{\nu-1} + d_2 y^{\nu-2} - \cdots \pm d_\nu = 0$$

sind, deren Coefficienten unserem Rationalitätsbereiche angehören. Die Gleichung (5) ist irreductibel.

Der letzte Satz muss noch bewiesen werden. Wir betrachten zu dem Zwecke denjenigen irreductiblen Factor $g_1(y)$ von $g(y)$, welcher den Nullwerth $y_1 = F(z_1)$ besitzt, und zeigen, dass er mit $g(y)$ selbst zusammenfallen muss, woraus dann natürlich die Irreductibilität von (5) folgt. Da $g_1(F(z_1)) = 0$ ist, so haben die beiden Gleichungen

$$g_1(F(z)) = 0 \quad \text{und} \quad f(z) = 0$$

eine Wurzel z_1 gemeinsam. Die zweite Gleichung ist der Voraussetzung nach irreductibel; also hat $g_1(F(z)) = 0$ alle Wurzeln von $f = 0$, und $g_1(y) = 0$ besitzt sicher die ν Wurzeln $y_1, y_2, \cdots y_\nu$. Diese sind unter einander verschieden, und daher steigt $g_1(y)$ zum Grade ν auf, d. h. es fällt mit $g(y)$ zusammen.

Jede symmetrische Function $S_1(z_1, \varphi(z_1), \cdots \varphi_{n-1}(z_1)) = F_1(z_1)$ kann rational durch $y_1 = S(z_1, \varphi(z_1), \cdots \varphi_{n-1}(z_1))$ dargestellt werden. Denn verstehen wir unter u eine unbestimmte Grösse und bilden nun die Summe

$$\frac{F_1(z_1)}{u - F(z_1)} + \frac{F_1(z_1')}{u - F(z_1')} + \cdots + \frac{F_1(z_1^{(\nu-1)})}{u - F(z_1^{(\nu-1)})} = \frac{1}{n} \sum_{\alpha=1}^{m} \frac{F_1(z_\alpha)}{u - F(z_\alpha)},$$

so zeigt die rechte Seite, dass dies eine symmetrische, gebrochene, rationale Function der Wurzeln von (1) ist. Es wird daher, nach Multiplication mit dem Polynome $g(u)$ von (5)

$$g(u)\left[\frac{F_1(z_1)}{u-F(z_1)}+\frac{F_1(z_1')}{u-F(z_1')}+\cdots+\frac{F_1(z_1^{(\nu-1)})}{u-F(z_1^{(\nu-1)})}\right]=G(u)$$

eine ganze Function von u mit rational bekannten Coefficienten. Trägt man hierin $u=y_1=F(z_1)$ ein, so erhält man als Resultat

$$F_1(z_1)=\frac{G(y_1)}{g'(y_1)}, \tag{6}$$

wobei g' die Ableitung von g bedeutet*). Damit ist der ausgesprochene Satz bewiesen. — Ebenso ist $F_1(z_1')=\frac{G(y_2)}{g'(y_2)}$, u. s. f.

§ 491. Nimmt man nun für $S_1=F_1$ der Reihe nach die elementaren symmetrischen Functionen von z_1, $\varphi(z_1)$, $\cdots$ $\varphi_{n-1}(z_1)$, so erhält man dadurch die Coefficienten derjenigen Gleichung, deren Wurzeln eben jene Grössen z_1, $\varphi(z_1)$, $\cdots$ sind, und da nach (6) die vorzunehmenden Rechnungen bei jedem der $(\nu-1)$ oberen Index von z_1 dieselben sind, so haben wir bewiesen: Die n Grössen $z_1^{(\alpha-1)}$, $\varphi(z_1^{(\alpha-1)})$, $\cdots$ $\varphi_{n-1}(z_1^{(\alpha-1)})$ (für $\alpha=1, 2, \cdots \nu$) sind die Wurzeln einer Gleichung

$$h(z;y_\alpha)\equiv z^n-\gamma_1(y_\alpha)\cdot z^{n-1}+\gamma_2(y_\alpha)\cdot z^{n-2}-\cdots\pm\gamma_n(y_\alpha)=0, \tag{7}$$

in welcher die γ_1, γ_2, $\cdots$ bestimmte rationale Functionen des Argumentes mit rational bekannten Coefficienten bedeuten. Es ist deshalb das Gleichungspolynom von (1) als Product darstellbar

$$f(z)=h(z;y_1)\cdot h(z;y_2)\cdots h(z;y_\nu), \tag{8}$$

d. h. wenn man nach Auflösung der Gleichung ν^{ten} Grades

$$g(y)\equiv y^\nu-d_1y^{\nu-1}+d_2y^{\nu-2}-\cdots\pm d_\nu=0 \tag{5}$$

sämmtliche Wurzeln y_1, y_2, $\cdots$ y_ν dem Rationalitätsbereiche hinzufügt, dann wird die vorher irreductible Function $f(z)$ reductibel und zerfällt nach (8) in ν Factoren desselben Grades $n=\frac{m}{\nu}$.

Das erhaltene Resultat können wir auch so deuten, dass wir die irreductible Gleichung

$$f(z)=0 \tag{1}$$

*) Diese Art der Herleitung stammt wohl von L. Kronecker (J. für Math. Bd. 91 (1881) S. 307).

als das Eliminationsresultat der Grösse y aus den beiden Gleichungen

$$(1^a) \qquad h(z, y) = 0 \quad \text{und} \quad g(y) = 0$$

auffassen. In der That stimmt ja (8) mit der in § 136, (4) Bd. I gegebenen Poisson'schen Darstellung der Resultanten vollkommen überein. Eine so darstellbare Gleichung (1) wollen wir eine imprimitive Gleichung nennen. Gleichungen (1), welche nicht die Eigenschaft haben, als Eliminationsresultat einer Grösse y aus zwei anderen Gleichungen (1^a) darstellbar zu sein, heissen primitive Gleichungen.

Die Gleichung (5) des abgeleiteten Theorems kann von ganz beliebigem Grade sein, so dass sie im Allgemeinen nur auflösbar werden wird, wenn die Zahl ν den Werth 4 nicht überschreitet, wie wir später zeigen werden.

§ 492. Wir gehen jetzt zu der Behandlung der besonderen, sogenannten cyklischen Gleichungen $h(z; y_\alpha) = 0$ über, für die also $\nu = 1$ ist. Eine cyklische Gleichung des Grades n ist eine solche, deren Wurzeln $z_1, z_2, \cdots z_n$ in die eine Reihe

$$(9) \qquad z_1, \quad z_2 = \varphi(z_1), \quad z_3 = \varphi_2(z_1), \quad \cdots \quad z_n = \varphi_{n-1}(z_1)$$

eingeordnet werden können, wobei φ eine rationale Function mit Coefficienten ist, die dem Rationalitätsbereiche angehören, und für welche $\varphi_n(z_1)$ die erste iterirte Function ist, die gleich z_1 wird.

Wir setzen fest, dass $z_h = z_k$ sein soll, wenn $h \equiv k \pmod{n}$ ist, so dass wir also auch höhere positive Indices als $(n-1)$ und auch negative bei z zulassen können. Ferner erinnern wir uns daran, dass es keine Beschränkung involvirt, φ als ganze Function vorauszusetzen. Zu erwähnen ist weiter, dass die Wurzeln $z_1, \cdots z_n$ auch in die Tabelle

$$(9^a) \quad z_\alpha, \quad z_{\alpha+1} = \varphi(z_\alpha), \quad z_{\alpha+2} = \varphi_2(z_\alpha), \quad \cdots \quad z_{\alpha-1} = \varphi_{n-1}(z_\alpha)$$

gebracht werden können, wobei α ein beliebiger Index ist.

Endlich zeigt die Anordnung (9), dass jede der Wurzeln der Gleichung eine rationale Function jeder anderen ist. Denn um z_α durch z_β darzustellen, reicht es aus, wenn $\beta + \gamma \equiv \alpha \pmod{n}$ ist, die Gleichung

$$\varphi_\gamma(z_\beta) = \varphi_\gamma(\varphi_{\beta-1}(z_1)) = \varphi_{\alpha-1}(z_1) = z_\alpha$$

anzusetzen. Diese beweist sofort die aufgestellte Behauptung.

Zunächst wollen wir, da Irreductibilität von $f(z) = h(z, y_\alpha)$ nicht in der Definition vorausgesetzt war, untersuchen, in welcher Weise unsere cyklische Gleichung $f(z) = h(z; y_\alpha) = 0$ reductibel sein kann. Es sei $f_1(z)$ derjenige irreductible Factor von $f(z)$, welcher den Wurzelfactor $(z - z_1)$ enthält. Ferner sei $z_{\alpha+1} = \varphi_\alpha(z_1)$ die erste unter den

Wurzeln in der Reihenfolge (9), die auch zu den Wurzeln der irreductiblen Gleichung $f_1(z) = 0$ gehört. Dann hat man durchaus die Verhältnisse, die wir in § 489 studirt haben; um dies einzusehen, braucht man nur das dortige φ hier durch φ_α zu ersetzen. Daher ordnen sich die Wurzeln von $f_1 = 0$ in eine Tabelle ein, die der Tabelle (4) entspricht. Die erste Zeile derselben wird

$$z_1, \quad \varphi_\alpha(z_1), \quad \varphi_{2\alpha}(z_1), \quad \cdots \quad \varphi_{\varkappa\alpha}(z_1); \qquad (\varphi_{\varkappa\alpha+\alpha}(z_1) = z_1).$$

Giebt es für $f_1(z) = 0$ noch andere Wurzeln, so kann eine zweite Zeile construirt werden; diese nimmt, weil alle Wurzeln in (9) enthalten sind, die Gestalt an

$$\varphi_\beta(z_1), \quad \varphi_{\alpha+\beta}(z_1), \quad \cdots \quad \varphi_{\varkappa\alpha+\beta}(z_1); \qquad (\varphi_{\varkappa\alpha+\alpha+\beta}(z_1) = \varphi_\beta(z_1)).$$

In dieser Art kann man fortfahren.

Nun sollte $\varphi_\alpha(z_1)$ die erste unter den Wurzeln (9) sein, die zu den Wurzeln von $f_1(z) = 0$ gehört. Folglich darf β nicht kleiner als α sein; läge aber β z. B. zwischen α und 2α, so läge $\varkappa\alpha + \beta$ zwischen $(\varkappa + 1)\alpha$ und $(\varkappa + 2)\alpha$; also könnte

$$\varkappa\alpha + \beta = (\varkappa + 1)\alpha + \gamma \qquad (\gamma < \alpha),$$

$$\varphi_{\varkappa\alpha+\beta}(z_1) = \varphi_\gamma[\varphi_{(\varkappa+1)\alpha}(z_1)] = \varphi_\gamma(z_1)$$

gesetzt werden, und man dürfte die zweite Zeile der Tabelle durch die ihr äquivalente

$$\varphi_\gamma(z_1), \quad \varphi_{\alpha+\gamma}(z_1), \quad \varphi_{2\alpha+\gamma}(z_1), \quad \cdots \qquad (\gamma < \alpha)$$

ersetzen. Das widerspricht der Annahme über α. Folglich erschöpft die erste Zeile der Tabelle bereits alle Wurzeln von $f_1 = 0$, und wir können schreiben

$$(10) \quad f_1(z) = (z - z_1)(z - \varphi_\alpha(z_1))(z - \varphi_{2\alpha}(z_1)) \cdots (z - \varphi_{(\mu-1)\alpha}(z_1)),$$
$$(\mu\alpha = n; \ \varphi_{\mu\alpha}(z_1) = z_1).$$

Ist dann $f_2(z)$ ein zweiter irreductibler Theiler von f, etwa derjenige, welcher den Factor $(z - \varphi(z_1))$ enthält, falls $\alpha > 1$ ist, so folgt, dass

$$f_1(z) = 0 \quad \text{und} \quad f_2(\varphi_1(z)) = 0$$

eine Wurzel gemeinsam haben; dass also $f_2(\varphi_1(z)) = 0$ alle Wurzeln von $f_1 = 0$ besitzt, und daher $f_2 = 0$ die Wurzeln $\varphi_1(z_1)$, $\varphi_{\alpha+1}(z_1)$, $\cdots$. Demnach ist f_2 von nicht geringerem Grade als f_1. Da auch das Umgekehrte gilt, wenn man

$$f_2(z) = 0 \quad \text{und} \quad f_1(\varphi_{n-1}(z)) = 0$$

betrachtet, so ergiebt sich, dass f_1 und f_2 von gleichem Grade sind. Es nimmt somit der zweite Factor die Form an

$$(10^a) \quad f_2(z) = (z - \varphi(z_1))(z - \varphi_{\alpha+1}(z_1)) \cdots (z - \varphi_{(\mu-1)\alpha+1}(z_1)).$$

Auf diese Weise sehen wir, dass eine etwa mögliche Zerfällung von $f(z)$ nur

$$(11)\qquad f(z)=f_1(z)f_2(z)\cdots f_\varrho(z)\cdots f_{\alpha-1}(z),$$

$$(12)\quad f_{\varrho+1}(z)=(z-\varphi_\varrho(z_1))\,(z-\varphi_{\alpha+\varrho}(z_1))\cdots(z-\varphi_{(\mu-1)\alpha+\varrho}(z_1)),$$
$$(\varrho=1,2,\cdots\alpha-1;\ \varphi_0(z_1)=z_1)$$

werden kann. Jeder irreductible Factor gleich Null gesetzt liefert also wieder eine cyklische Gleichung. Wir können demnach ohne Beschränkung von vornherein voraussetzen, dass die vorgelegte cyklische Gleichung irreductibel sei.

§ 493. Die bei der Kreistheilungsgleichung besprochene Gauss'sche Methode führt uns auch hier zu den Elementen der algebraischen Lösung. Es sei der Grad der cyklischen, irreductiblen Gleichung

$$(13)\qquad f(z)\equiv z^n-c_1z^{n-1}+c_2z^{n-2}-\cdots=0$$

eine zusammengesetzte Zahl $n=k\cdot l$. Die Wurzeln $z_1,\varphi(z_1),\cdots\varphi_{n-1}(z_1)$ ordnen wir in folgende Tabelle ein, indem wir $\varphi(z_1)=z_2$, $\varphi_2(z_1)=z_3$, $\cdots\ \varphi_{k-1}(z_1)=z_k$ setzen,

$$(14)\qquad \begin{array}{llllll} z_1, & \varphi_k(z_1), & \varphi_{2k}(z_1), & \cdots & \varphi_{(l-1)k}(z_1) & \\ z_2, & \varphi_k(z_2), & \varphi_{2k}(z_2), & \cdots & \varphi_{(l-1)k}(z_2) & (z_2=\varphi(z_1)) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ z_k, & \varphi_k(z_k), & \varphi_{2k}(z_k), & \cdots & \varphi_{(l-1)k}(z_k) & (z_k=\varphi_{k-1}(z_1)). \end{array}$$

Wir wählen wieder eine allgemeine, symmetrische Function

$$(15)\quad S(z_\alpha,\varphi_k(z_\alpha),\cdots\varphi_{(l-1)k}(z_\alpha))=F(z_\alpha)=F(\varphi_k(z_\alpha))=\cdots=y_\alpha$$
$$(\alpha=1,2,\cdots k),$$

für welche $y_1, y_2, \cdots y_k$ von einander verschieden ausfallen. Dann ergiebt sich genau wie in § 490 ff., dass die y einer irreductiblen Gleichung k^{ten} Grades

$$(5^a)\qquad g(y)\equiv y^k-d_1y^{k-1}+d_2y^{k-2}-\cdots$$
$$=(y-y_1)\,(y-y_2)\cdots(y-y_k)=0$$

genügen, deren Coefficienten dem Rationalitätsbereiche angehören, und dass die Elemente der α^{ten} Zeile von (14) Wurzeln einer cyklischen Gleichung l^{ten} Grades werden, deren Coefficienten rational von y_α abhängen:

$$(7^a)\qquad h(z;y_\alpha)=(z-z_\alpha)\,(z-\varphi_k(z_\alpha))\cdots(z-\varphi_{(l-1)k}(z_\alpha))$$
$$(\alpha=1,2,\cdots k).$$

Um alle z_α zu finden, reicht es aber aus, eine einzige der Gleichungen (7^a) zu lösen, ja sogar auch nur eine Wurzel einer derselben zu bestimmen;

denn mit irgend einem z_α sind die übrigen Wurzeln $\varphi(z_\alpha)$, $\varphi_2(z_\alpha)$, $\cdots$ $\varphi_{n-1}(z_\alpha)$ von (13) als rationale Functionen von z_α auch gegeben.

Diese Resultate stimmen mit den früheren überein; als neuer Umstand kommt aber noch dazu, dass die Gleichung (5^a) ebenfalls eine cyklische Gleichung ist, während im früheren allgemeinen Falle die Gleichung (5) dieser Einschränkung nicht unterworfen war.

Um die ausgesprochene neue Eigenschaft herzuleiten, bringen wir die Functionen y_2, y_3, $\cdots$ auf die Formen

$$y_2 = F(z_2) = F(\varphi(z_1)), \quad y_3 = F(z_3) = F(\varphi(z_2)), \quad \cdots \quad y_1 = F(\varphi(z_n));$$

dann wird, wenn u eine Unbestimmte bedeutet,

$$\frac{y_2}{u-y_1} = \frac{F(\varphi(z_1))}{u-F(z_1)} = \frac{F(\varphi_{k+1}(z_1))}{u-F(\varphi_k(z_1))} = \frac{F(\varphi_{2k+1}(z_1))}{u-F(\varphi_{2k}(z_1))} = \cdots,$$

und also ergiebt sich die Summe

$$\frac{y_2}{u-y_1} + \frac{y_3}{u-y_2} + \cdots + \frac{y_1}{u-y_k}$$
$$= \frac{1}{l}\left[\frac{F(\varphi(z_1))}{u-F(z_1)} + \frac{F(\varphi_2(z_1))}{u-F(\varphi_1(z_1))} + \cdots + \frac{F(\varphi_n(z_1))}{u-F(\varphi_{n-1}(z_1))}\right]$$

als gebrochene, symmetrische Function sämmtlicher Wurzeln z_1, $\varphi(z_1)$; $\cdots$ $\varphi_{n-1}(z_1)$; denn die rechte Seite ändert sich nicht, wenn man statt z_1 irgend eine andere Wurzel einträgt.

Multipliciren wir jetzt diesen letzten Ausdruck mit dem in den z_1, $\varphi(z_1)$, $\cdots$ gleichfalls symmetrischen Polygone $g(u)$ aus (5^a), dann wird das Product

$$g(u)\left[\frac{y_2}{u-y_1} + \frac{y_3}{u-y_2} + \cdots + \frac{y_1}{u-y_k}\right] = G(u)$$

eine ganze Function von u und eine ganze, symmetrische Function der Wurzeln von (13). Also ist $G(u)$ rational darstellbar. Trägt man hierin $u = y_1, y_2, \cdots y_k$ ein, so verschwinden jedesmal alle Glieder der linken Seite bis auf eins, und es folgt die Werthbestimmung für die y_2, y_3, $\cdots$

$$(16) \qquad y_2 = \frac{G(y_1)}{g'(y_1)}, \quad y_3 = \frac{G(y_2)}{g'(y_2)}, \quad \cdots \quad y_1 = \frac{G(y_k)}{g'(y_k)}.$$

Diese Relationen zwischen den Wurzeln von (5^a) sind charakteristisch dafür, dass (5^a) eine cyklische Gleichung ist.

Hiermit haben wir die folgenden Resultate bewiesen: Die vollständige Lösung einer cyklischen Gleichung (13) des Grades $n = kl$ kann dadurch bewerkstelligt werden, dass man eine Wurzel einer cyklischen Gleichung (5^a) des Grades k ermittelt; mit ihrer Hülfe die Coefficienten einer anderen

cyklischen Gleichung (7^a) des Grades l auf rationalem Wege bestimmt, und endlich auch noch eine Wurzel dieser letzten Gleichung des Grades l aufsucht.

Sind k und l Primzahlen, dann hat unsere Reduction ihr Ende erreicht; ist aber auch nur einer der Factoren eine zusammengesetzte Zahl, so können wir auf die entsprechende Gleichung dieselbe Reduction anwenden. So sehen wir: Ist n in seine gleichen oder verschiedenen Primfactoren zerlegt $= p_1 \cdot p_2 \cdots p_\varkappa$, dann hängt die vollständige Auflösung der cyklischen Gleichung des Grades (13) von der aufeinander folgenden Bestimmung je einer Wurzel je einer cyklischen Gleichung des Primzahlgrades $p_1, p_2, \cdots p_\varkappa$ ab. Durch die Bestimmung der Wurzel einer dieser Gleichungen werden die Coefficienten der nächstfolgenden cyklischen Gleichung festgelegt. Die Anordnung der p kann dabei völlig willkürlich getroffen werden.

Nach der in § 491 eingeführten Terminologie können wir sagen: Jede cyklische Gleichung, deren Grad keine Primzahl ist, gehört zu den imprimitiven Gleichungen.

§ 494. Nach unseren bisherigen Schlüssen wären wir berechtigt, die Gradzahl einer vorgelegten cyklischen Gleichung als Primzahl anzunehmen und uns auf die Auflösung solcher Primzahlgleichungen zu beschränken. Wir brauchen diese Voraussetzung aber bei der nun zu besprechenden Lagrange'schen Methode nicht zu machen, ebenso wenig wie dies an der gleichen Stelle bei der Behandlung der Kreistheilungsgleichungen nöthig war; und wir werden daher über die Gradzahl n keine beschränkenden Voraussetzungen zu Grunde legen.

Wir verstehen unter α irgend eine n^{te} Einheitswurzel, bilden mit ihrer Hülfe die Lagrange'schen Resolventen für die n Wurzeln z_1, $z_2, \cdots z_n$ von (13)

$$(17)\quad \begin{aligned}(z_\lambda;\alpha) &= z_\lambda + \alpha z_{\lambda+1} + \alpha^2 z_{\lambda+2} + \cdots + \alpha^{n-1} z_{\lambda-1}\\ &= z_\lambda + \alpha\varphi(z_\lambda) + \alpha^2\varphi_2(z_\lambda) + \cdots + \alpha^{n-1}\varphi_{n-1}(z_\lambda)\end{aligned} \quad (\lambda = 1, 2, \cdots n)$$

und finden für sie die fundamentale Beziehung (§ 321, Bd. I)

$$(18)\quad (z_{\lambda+1};\alpha) = z_{\lambda+1} + \alpha z_{\lambda+2} + \alpha^2 z_{\lambda+3} + \cdots + \alpha^{n-1} z_\lambda = \alpha^{-1}(z_\lambda;\alpha).$$

Aus dieser geht sofort hervor, da $\alpha^n = 1$ ist,

$$(z_{\lambda+1};\alpha)^n = (z_\lambda;\alpha)^n,$$

und demnach gilt für diese Potenz der Resolvente die Gleichungsreihe

$$(19)\quad (z_1;\alpha)^n = (z_2;\alpha)^n = \cdots = (z_n;\alpha)^n.$$

Wir sind daher im Stande, $(z_1; \alpha)^n$ als symmetrische Function sämmtlicher Wurzeln z darzustellen; es giebt eine rationale Function $T(\alpha)$ von α mit Coefficienten, die dem Rationalitätsbereiche angehören, so dass

$$(z_1; \alpha)^n = \frac{1}{n}[(z_1; \alpha)^n + (z_2; \alpha)^n + \cdots + (z_n; \alpha)^n] = T(\alpha).$$

Durch Ausziehung der n^{ten} Wurzel erhalten wir aus dieser und aus den entsprechenden Gleichungen für $\alpha^2, \alpha^3, \cdots \alpha^{n-1}$ das folgende System linearer Gleichungen mit den Unbekannten $z_1, z_2, \cdots z_n$:

$$\begin{aligned}
&z_1 + \alpha z_2 \quad + \alpha^2 z_3 \quad + \cdots + \alpha^{n-1} z_n \;\; = \sqrt[n]{T(\alpha)},\\
&z_1 + \alpha^2 z_2 \quad + \alpha^4 z_3 \quad + \cdots + \alpha^{2(n-1)} z_n = \sqrt[n]{T(\alpha^2)},\\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\\
&z_1 + \alpha^{n-1} z_2 + \alpha^{2n-2} z_3 + \cdots + \alpha^{(n-1)^2} z_n = \sqrt[n]{T(\alpha^{n-1})}.
\end{aligned}$$

Wir nehmen jetzt α als primitive n^{te} Einheitswurzel an, damit alle diese Ausdrücke formal von einander verschieden seien. Fügen wir zu jenen Gleichungen die aus (13) folgende n^{te} lineare Gleichung

$$z_1 + z_2 + z_3 + \cdots + z_n = (z; 1) = c_1,$$

so ergiebt sich durch geeignete Combination als Lösung der cyklischen Gleichung

$$\begin{aligned}
n z_1 &= c_1 + \sum_{\varkappa=1}^{n-1} \sqrt[n]{T(\alpha^\varkappa)} &&= c_1 + \sum_{\varkappa=1}^{n-1} (z_1; \alpha^\varkappa),\\
n z_2 &= c_1 + \sum_{\varkappa=1}^{n-1} \alpha^{-\varkappa} \sqrt[n]{T(\alpha^\varkappa)} &&= c_1 + \sum_{\varkappa=1}^{n-1} \alpha^{-\varkappa} (z_1; \alpha^\varkappa),\\
n z_3 &= c_1 + \sum_{\varkappa=1}^{n-1} \alpha^{-2\varkappa} \sqrt[n]{T(\alpha^\varkappa)} &&= c_1 + \sum_{\varkappa=1}^{n-1} \alpha^{-2\varkappa} (z_1; \alpha^\varkappa),\\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot
\end{aligned} \tag{20}$$

§ 495. Diese Formeln (20) bergen einen Missstand, der darin beruht, dass jede der in die rechten Seiten eingehenden n^{ten} Wurzeln n Werthe hat, ohne dass über die Combination dieser Werthe etwas ausgesagt ist, so dass also die erste Formel in (20) nicht, wie es sein müsste, gerade die gesuchten n Werthe, sondern im Ganzen n^{n-1} Werthe besitzt. Ausser den Wurzeln von (13) werden also noch $(n^{n-1} - n)$ fremde Werthe durch (20) dargestellt.

Diesem Mangel lässt sich auf folgende Art abhelfen. Aus (18) ersieht man wegen

$$\begin{aligned}
(z_{\lambda+1}; \alpha^\varkappa)\,(z_{\lambda+1}; \alpha)^{-\varkappa} &= [\alpha^{-\varkappa} \cdot (z_\lambda; \alpha^\varkappa)]\,[\alpha^{-1} \cdot (z_\lambda; \alpha)]^{-\varkappa}\\
&= (z_\lambda; \alpha^\varkappa)\,(z_\lambda; \alpha)^{-\varkappa},
\end{aligned}$$

dass auch der Ausdruck auf der linken Seite symmetrisch in den z ist, wie dies oben bei $(z_\lambda;\alpha)^n$ der Fall war. Man kann ihn daher als rationale Function von α mit rationalen Coefficienten ausdrücken. Wir wollen diese Darstellung mit $T_\varkappa$ bezeichnen, und setzen somit

$$(21)\qquad (z_\lambda;\alpha^\varkappa)(z_\lambda;\alpha)^{-\varkappa}=T_\varkappa;\quad (z_\lambda;\alpha^\varkappa)=T_\varkappa\cdot(z_\lambda;\alpha)^\varkappa.$$

Demgemäss wird, wenn wir statt $T(\alpha)$ kürzer T schreiben,

$$(21^a)\qquad (z_\lambda;\alpha^2)=T_2\sqrt[n]{T^2},\quad (z_\lambda;\alpha^3)=T_3\sqrt[n]{T^3},\quad\cdots$$

und aus (20) folgt, wenn man diese Werthe einträgt,

$$(20^a)\qquad \begin{aligned} nz_1&=c_1+\sqrt[n]{T}+T_2\sqrt[n]{T^2}+T_3\sqrt[n]{T^3}+\cdots,\\ nz_2&=c_1+\alpha^{-1}\sqrt[n]{T}+\alpha^{-2}T_2\sqrt[n]{T^2}+\alpha^{-3}T_3\sqrt[n]{T^3}+\cdots,\\ nz_3&=c_1+\alpha^{-2}\sqrt[n]{T}+\alpha^{-4}T_2\sqrt[n]{T^2}+\alpha^{-6}T_3\sqrt[n]{T^3}+\cdots,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots. \end{aligned}$$

Alle T sind rationale Functionen; jede der Formen ist eindeutig bestimmt, sobald der Werth für $\sqrt[n]{T}$ festgelegt ist; ändert man ihn, was nur so möglich ist, dass ein Factor α^λ dazutritt, dann gehen die Zeilen in (20^a) nur in einander über; die erste Zeile kann als n-deutiger Ausdruck aufgefasst werden, welcher sämmtliche n Wurzeln liefert. Damit ist die ausgesprochene Schwierigkeit überwunden.

§ 496. Es kann aber bei der Benutzung von (21), (21^a) eine andere Schwierigkeit entstehen. α bedeutet irgend eine primitive n^{te} Einheitswurzel; es könnte für jeden der $\varphi(n)$ Werthe α die Resolvente $(z_\lambda;\alpha)$ zu Null werden, so dass in (21) der Werth von $T_\varkappa$ in unbestimmter Form aufträte. Ja es reicht, um diesen Fall herbeizuführen, schon aus, dass für ein primitives α die Resolvente verschwindet. Denn hat die Gleichung

$$(z_1;t)=z_1+z_2t+\cdots+z_nt^{n-1}=0$$

eine primitive n^{te} Einheitswurzel $t=\alpha$ zur Wurzel, dann besitzt sie alle.

Bei $n=p^\varkappa$ kann diese Schwierigkeit nicht eintreten. Denn setzen wir $n=p\cdot q$ also $q=p^{\varkappa-1}$ und ferner

$$\begin{aligned} n(z_{q+1}-z_1)=[(\alpha^{-q}-1)(z_1;\alpha)+(\alpha^{-2q}-1)(z_1;\alpha^2)\\ +\cdots+(\alpha^{-pq}-1)(z_1;\alpha^q)]+[(\alpha^{-pq-1}-1)(z_1;\alpha^{q+1})\\ +\cdots+(\alpha^{-2pq}-1)(z_1;\alpha^{2q})]+\cdots, \end{aligned}$$

so kann, falls die Gleichung in z irreductibel ist, die linke Seite nicht $=0$ sein. Rechts verschwindet das Schlussglied jeder eckigen Klammer,

weil xpq ein Vielfaches von n ist. Es können also nicht alle übrigen Resolventen $(z_1; \alpha^\lambda)$ Null sein; die zugehörigen α^λ gehören aber zu den primitiven Wurzeln. Wir entgehen also dieser Möglichkeit, wenn wir, was nach § 493 erlaubt ist, n als Primzahlpotenz annehmen.

Aber auch im allgemeinen Falle kann man jenem Uebelstande abhelfen, indem man, wie H. Weber es thut*), alle z_λ durch eine und dieselbe nicht verschwindende n-deutige Function ausdrückt.

Es sei n durch die Primzahl p theilbar, und zwar $n = pq$. Dann können wir auch bei diesem allgemeineren q aus der letzten Gleichung in der angegebenen Weise schliessen, dass ein nicht verschwindendes $(z_1; \alpha^x)$ mit einem zu p theilerfremden Exponenten x vorhanden ist.

Nun sei, in seine verschiedenen Primzahlpotenzen zerlegt,

$$n = p_1^\alpha p_2^\beta p_3^\gamma \cdots = p_1^\alpha q_1 = p_2^\beta q_2 = p_3^\gamma q_3 = \cdots;$$

dann bestimmen wir nicht verschwindende Resolventen

$$(z_\lambda; \alpha^{\mu_1}), \quad (z_\lambda; \alpha^{\mu_2}), \quad (z_\lambda; \alpha^{\mu_3}), \quad \cdots$$

für welche μ_1 theilerfremd zu p_1, ebenso μ_2 zu p_2, $\cdots$ ist. Hieraus bilden wir mit willkürlichem x und noch unbestimmtem x_0 das Product

$$(22) \qquad (z_\lambda; \alpha^x)\,[(z_\lambda; \alpha^{\mu_1})^{q_1} (z_\lambda; \alpha^{\mu_2})^{q_2} (z_\lambda; \alpha^{\mu_3})^{q_3} \cdots]^{-x_0}.$$

Ersetzen wir hierin λ durch $(\lambda + 1)$, so bleibt nach (18) der Werth des Ausdruckes (22) unverändert, falls

$$(22^a) \qquad x \equiv x_0(\mu_1 q_1 + \mu_2 q_2 + \mu_3 q_3 + \cdots) \pmod{n}$$

wird. Nun ist die Klammer theilerfremd zu n, wie man leicht sieht. Demnach kann man zu jedem x ein x_0 gemäss (22^a) bestimmen. Für dieses x_0 ist (22) symmetrisch in den z und mit Hülfe von α rational darstellbar. Wir bezeichnen (22) mit $U_x(\alpha)$ oder kürzer mit U_x. Ferner ist die n^{te} Potenz der eckigen Klammer in (22) nach (19) symmetrisch in den z; wir bezeichnen sie mit $V(\alpha)$ oder kürzer mit V. Diese Function verschwindet nicht.

Dann gilt für jeden Exponenten x die Gleichung

$$(23) \qquad (z_\lambda; \alpha^x) = U_x V^{\frac{x_0}{n}},$$

und durch Substitution dieser Werthe in (20) ergiebt sich die Form

*) Algebra I; zweite Aufl. § 172.

$$(20^b)\qquad \begin{aligned} n z_1 &= c_1 + \sum_{\varkappa=1}^{n-1} U_\varkappa \sqrt[n]{V^{\varkappa_0}},\\ n z_2 &= c_1 + \sum_{\varkappa=1}^{n-1} \alpha^{-\varkappa} U_\varkappa \sqrt[n]{V^{\varkappa_0}},\\ n z_3 &= c_1 + \sum_{\varkappa=1}^{n-1} \alpha^{-2\varkappa} U_\varkappa \sqrt[n]{V^{\varkappa_0}},\\ &\cdots\cdots\cdots\cdots \end{aligned}$$

durch welche die angegebene Schwierigkeit überwunden ist.

§ 497. Wir machten soeben darauf aufmerksam, dass $V(\alpha)$ eine rational darstellbare Grösse sei; setzen wir sie in die Normalform complexer Ausdrücke gemäss der Bezeichnung aus § 7, Bd. I

$$V(\alpha) = R \cdot \left[{}^c_s\, \Theta\right],$$

so wird

$$(24)\qquad V(\alpha)^{\frac{1}{n}} = R^{\frac{1}{n}} \cdot \left[{}^c_s\, \frac{1}{n}\Theta\right],$$

wobei R und Θ rational bekannt sind.

Abel*) hat gezeigt, dass bei vorgelegtem reellen Rationalitätsbereiche die Ausziehung der n^{ten} Wurzel sich durch einfachere Operationen ersetzen lässt. Schreiben wir

$$\alpha = \left[{}^c_s\, \varphi\right]$$

für die benutzte primitive Einheitswurzel, dann entsteht, da dies das einzige in V als complex eingehende Element ist,

$$V(\alpha) = g_0 + g_1 \cdot \left[{}^c_s\, \varphi\right] + g_2 \cdot \left[{}^c_s\, 2\varphi\right] + \cdots$$

bei reellen Coefficienten g. Daraus ergiebt sich

$$\begin{aligned} V(\alpha^{-1}) &= g_0 + g_1 \cdot \left[{}^c_s - \varphi\right] + g_2 \cdot \left[{}^c_s - 2\varphi\right] + \cdots,\\ |V(\alpha)| = |V(\alpha^{-1})| &= [(g_0 + g_1 \cos\varphi + \cdots)^2\\ &\qquad + (g_1 \sin\varphi + g_2 \sin 2\varphi + \cdots)^2]^{\frac{1}{2}}, \end{aligned}$$

d. h. $|V(\alpha)| = |V(\alpha^{-1})|$ und $= R$. Hieraus folgt sofort

$$V(\alpha^{-1}) = R \cdot \left[{}^c_s - \Theta\right],$$

$$(24^a)\qquad V(\alpha^{-1})^{\frac{1}{n}} = R^{\frac{1}{n}} \cdot \left[{}^c_s - \frac{1}{n}\Theta\right].$$

---

*) Oeuvres, éd. Sylow et Lie, 1; p. 493.

Ferner ist nach (18)

$$\begin{aligned}&[(z_{\lambda+1};\alpha^{\mu_1})^{q_1}\cdots][(z_{\lambda+1};\alpha^{-\mu_1})^{q_1}\cdots]\\&\qquad=[\alpha^{-\mu_1 q_1}(z_\lambda;\alpha^{\mu_1})^{q_1}\cdots][\alpha^{\mu_1 q_1}(z_\lambda;\alpha^{-\mu_1})^{q_1}\cdots]\\&\qquad=[(z_\lambda;\alpha^{\mu_1})^{q_1}\cdots][(z_\lambda;\alpha^{-\mu_1})^{q_1}\cdots],\end{aligned}$$

so dass dieser Ausdruck in den z symmetrisch wird, und wir

$$V(\alpha)^{\frac{1}{n}}\,V(\alpha^{-1})^{\frac{1}{n}}=Q$$

setzen können, wobei Q eine rational bekannte Grösse bedeutet.

Verbindet man hiermit das aus (24) und (24*) folgende Resultat

$$V(\alpha)^{\frac{1}{n}}\,V(\alpha^{-1})^{\frac{1}{n}}=R^{\frac{2}{n}},$$

so ergiebt sich

$$R^{\frac{1}{n}}=\sqrt{Q},$$

und also

$$V(\alpha)^{\frac{1}{n}}=\sqrt{Q}\left[{c \atop s}\,\frac{1}{n}\Theta\right],$$

d. h.: **Ist der Rationalitätsbereich der cyklischen Gleichung reell, dann kann ihre Auflösung so durchgeführt werden, dass man aus einer, nach Adjunction einer primitiven n^{ten} Einheitswurzel bekannten, reellen Grösse Q die zweite Wurzel auszieht und einen bekannten Winkel in n gleiche Theile theilt.**

Abel macht ferner darauf aufmerksam, dass in einem reellen Bereiche die Realitätsverhältnisse der Wurzeln leicht zu überblicken seien. Ist nämlich $z_\varkappa$ eine reelle Wurzel, so sind $\varphi(z_\varkappa)$, $\varphi_2(z_\varkappa)$, $\cdots$ d. h. auch alle anderen Wurzeln reell. Demnach besitzt hier jede cyklische Gleichung entweder nur reelle oder nur complexe Wurzeln. Natürlich gehören die Gleichungen ungeraden Grades zu der ersten Art.

§ 498. Jede Gleichung zweiten Grades

$$z^2-c_1z+c_2=0$$

ist cyklisch; denn man hat ja, wenn z_1, z_2 ihre Wurzeln bedeuten,

$$z_2=\varphi(z_1)=c_1-z_1,\quad z_1=\varphi(z_2)=c_1-z_2.\ —$$

Die allgemeinen Gleichungen dritten Grades sind nicht cyklisch, wenn man zum Rationalitätsbereiche nur ihre Coefficienten nimmt. Erweitert man ihn jedoch durch Hinzunahme der Quadratwurzel aus der Discriminante $\sqrt{D}$, so wird die Gleichung dritten Grades

$$z^3-c_1z^2+c_2z-c_3\equiv f(z)=0$$

mit den Wurzeln z_1, z_2, z_3 cyklisch. Denn es ist in diesem Falle

$$(z_1 - z_2)(z_1 - z_3)(z_2 - z_3) = \sqrt{D};$$

$$z_2 - z_3 = \frac{\sqrt{D}}{f'(z_1)}, \qquad z_2 + z_3 = c_1 - z_1;$$

$$z_2 = \frac{1}{2}\left(c_1 - z_1 + \frac{\sqrt{D}}{f'(z_1)}\right),$$

oder, wenn man in bekannter Weise umwandelt,

$$z_2 = \frac{1}{2\sqrt{D}}\Big\{(2c_1^2 - 6c_2)z_1^2 - (2c_1^3 - 7c_1c_2 + 9c_3 + \sqrt{D})z_1 + (c_1^2c_2 + 3c_1c_3 - 4c_2^2 + c_1\sqrt{D})\Big\}\cdot —$$

Dass die Kreistheilungsgleichungen cyklisch seien, haben wir schon hervorgehoben. —

Zu anderen cyklischen Gleichungen können wir durch den Satz gelangen, dass jede rationale Function der Wurzeln einer irreductiblen cyklischen Gleichung selbst die Wurzel einer cyklischen Gleichung ist. Wir deuten den einfachen Beweis kurz an.

Zuerst reicht es aus, eine einzige Wurzel zu Grunde zu legen, da jede andere durch die eine gewählte z_1 rational darstellbar ist. Es sei $G(z_1)$ eine ganze rationale Function von z_1, und es seien

$$G(z_1), \quad G(\varphi(z_1)), \quad G(\varphi_2(z_1)), \quad \cdots \quad G(\varphi_{n-1}(z_1))$$

ihre Werthe für die Wurzeln der cyklischen Gleichung. Durch unsere früher verwendeten Schlüsse erkennt man, dass, wenn diese n Werthe nicht sämmtlich von einander verschieden sind, sondern etwa $G(z_1) = G(\varphi_k(z_1))$ ist, eine Anordnung

$$\begin{array}{llll} G(z_1), & G(\varphi(z_1)), & \cdots & G(\varphi_{k-1}(z_1)), \\ G(\varphi_k(z_1)), & G(\varphi_{k+1}(z_1)), & \cdots & G(\varphi_{2k-1}(z_1)), \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \end{array}$$

getroffen werden kann, bei welcher die Elemente jeder Spalte untereinander gleich, dagegen die einer Zeile sämmtlich von einander verschieden sind. Zugleich werden dabei die Elemente einer Zeile zu Wurzeln einer irreductiblen Gleichung

$$k(u) \equiv (u - G(z_1))(u - G(\varphi(z_1))) \cdots (u - G(\varphi_{k-1}(z_1))) = 0,$$

deren Coefficienten dem Rationalitätsbereiche angehören; und die Betrachtung von

$$k(u)\left[\frac{G(\varphi(z_1))}{u - G(z_1)} + \frac{G(\varphi(z_2))}{u - G(z_2)} + \cdots + \frac{G(\varphi(z_{k-1}))}{u - G(z_{k-1})}\right]$$

zeigt wie oben, dass

$$G(\varphi(z_1)) = \chi(G(z_1)), \quad G(\varphi_2(z_1)) = \chi(G(\varphi(z_1))), \quad \cdots$$

wird, wobei χ eine rationale Function bezeichnet. Damit ist aber der ausgesprochene Satz bewiesen. —

Hiernach ist jede rationale Function einer Einheitswurzel wiederum die Wurzel einer cyklischen Gleichung. Bedeutet z. B. ω eine primitive fünfte Einheitswurzel, und setzen wir

$$y_1 = 1 + \omega + \omega^2, \quad y_2 = 1 + \omega^2 + \omega^4,$$
$$y_3 = 1 + \omega^4 + \omega^3, \quad y_4 = 1 + \omega^3 + \omega,$$

dann müssen nach unseren Ueberlegungen rationale Grössen a, b, c, d, e existieren, für welche man hat

$$1 + \omega^2 + \omega^4 = a(1 + \omega + \omega^2)^4 + b(1 + \omega + \omega^2)^3 + c(1 + \omega + \omega^2)^2$$
$$+ d(1 + \omega + \omega^2) + e;$$

die Methode der unbestimmten Coefficienten liefert in der That die Werthe

$$a = 0, \quad b = 2, \quad c = -3, \quad d = 6, \quad e = -2.$$

Ferner wird die Gleichung $(y - y_1) \cdots (y - y_4) = 0$ gefunden mit Hülfe von

$$\sum y_\alpha = 2, \quad \sum y_\alpha^2 = -4, \quad \sum y_\alpha^3 = -7, \quad \sum y_\alpha^4 = 4,$$

in der Form

$$y^4 - 2y^3 + 4y^2 - 3y + 1 = 0;$$

und hier ist also gemäss der Bestimmung der $a, b, \cdots e$

$$y_2 = \varphi(y_1) = 2y_1^3 - 3y_1^2 + 6y_1 - 2.$$

Es ergiebt sich daraus durch Potenziren und Vereinfachen

$$y_2^2 = 2y_1^3 - 4y_1^2 + 7y_1 - 5,$$
$$y_2^3 = -3y_1^3 + 3y_1^2 - 8y_1,$$
$$y_2^4 = -8y_1^3 + 13y_1^2 - 26y_1 + 13;$$

trägt man diese Werthe für $y_2, y_2^2, \cdots y_2^4$ in die Gleichung für y ein, so wird in der That $y_2^4 - 2y_2^3 + 4y_2^2 - 3y_2 + 1 = 0$, wie die Eigenschaft der cyklischen Gleichungen es forderte.

§ 499. Eine andere Methode für die Herstellung cyklischer Gleichungen ist die folgende. Die Wurzeln der irreductiblen cyklischen Gleichung $f(z) = 0$ seien

$$z_1, \quad \varphi(z_1), \quad \varphi_2(z_1), \quad \cdots \quad \varphi_{n-1}(z_1),$$

und $\varphi_n(z_1)$ sei die erste iterirte Function, welche den Anfangswerth z_1 wieder annimmt. Dann hat $\varphi_n(z) - z = 0$ mit $f(z) = 0$ eine Wurzel z_1

gemeinsam, und wegen der vorausgesetzten Irreductibilität von $f = 0$ ist also $f(z)$ ein Theiler von $\varphi_n(z) - z$. Das lässt sich noch präcisiren. Wenn ζ eine Wurzel von $\varphi(z) - z = 0$ ist, dann hat man auch $\varphi_2(\zeta) = \varphi(\zeta) = \zeta, \cdots \varphi_n(\zeta) = \zeta$, und also ist ζ zwar eine Wurzel von $\varphi_n(z) - z = 0$, aber wegen der über n gemachten Voraussetzung nicht von $f(z) = 0$. Wir erkennen daher (vgl. § 270, Bd. I), dass

$$\frac{\varphi_n(z) - z}{\varphi(z) - z} \tag{25}$$

eine ganze Function von z, und dass $f(z)$ ein Theiler derselben wird. Falls n eine Primzahl ist, können wir nicht über (25) hinausgehen; bedeutet n eine zusammengesetzte Zahl, so können wir ähnliche Schlüsse anwenden, wie bei der Herstellung der Gleichung, welche die primitiven n^{ten} Einheitswurzeln liefert.

Hierbei wird es nothwendig, vorauszusetzen, dass die Coefficienten der Function $\varphi(z)$ unbestimmte Grössen seien, um behaupten zu können, dass $\varphi_n(z) - z = 0$ keine mehrfachen Wurzeln enthält; (der ähnliche Umstand wurde ja auch bei der Kreistheilungsgleichung benutzt). Gäbe es nun auch im allgemeinen Falle mehrfache Wurzeln, so müsste dies ebenso bei der besonderen Wahl der Function φ

$$\varphi(z) = z^{\mu}, \quad \varphi_2(z) = z^{\mu^2}, \quad \cdots \quad \varphi_n(z) = z^{\mu^n},$$
$$\varphi_n(z) - z = z(z^{\mu^n - 1} - 1)$$

eintreten; da kommen aber gleiche Wurzeln nicht vor (§ 294, Bd. I).

In besonderen Fällen kommen wirklich mehrfache Wurzeln vor. Setzt man z. B.

$$\varphi(z) = z^2 - \frac{3}{4}, \qquad \varphi_2(z) = z^4 - \frac{3}{2} z^2 - \frac{3}{16},$$

dann wird

$$\varphi_2(z) - z = z^4 - \frac{3}{2} z^2 - z - \frac{3}{16} = \left(z + \frac{1}{2}\right)^3 \left(z - \frac{3}{2}\right).$$

Wenn nun z_x eine Wurzel von $\varphi_n(z) - z = 0$ ist, so wird ein Glied der Reihe, die wir beliebig weit fortgesetzt denken,

$$z_x, \quad \varphi(z_x), \quad \varphi_2(z_x), \quad \cdots$$

wieder gleich z_x. Ist $\varphi_d(z_x)$ das erste dieser Eigenschaft, so wollen wir sagen, z_x gehört zum Exponenten d. Nach bekannter Schlussweise leitet man ab: Jeder Exponent, zu dem eine Wurzel gehört, ist ein Theiler von n. Ferner nennen wir eine Wurzel primitiv, wenn sie zum Exponenten n gehört. Ist also n eine Primzahl, so giebt es nur Wurzeln, die zu 1 oder die zu n gehören,

und weil keine vielfachen Wurzeln vorhanden sind, so hat (25) nur noch primitive Wurzeln.

Um den allgemeinen Fall bequem schreiben zu können, setzen wir

$$\varphi_{\mu:\tau}(z) - z = [\mu:\tau].$$

Ist nun die Gradzahl in ihre Primzahlpotenzen zerlegt

$$n = p_1^{\nu_1} p_2^{\nu_2} p_3^{\nu_3} \cdots p_\varkappa^{\nu_\varkappa},$$

dann wird die Gleichung

$$(26) \qquad \Phi_n(z) \equiv \frac{[n:1][n:p_1p_2][n:p_1p_3][n:p_2p_3]\cdots}{[n:p_1][n:p_2][n:p_3]\cdots[n:p_1p_2p_3]\cdots} = 0$$

alle und nur die primitiven Wurzeln von $\varphi_n(z) - z = 0$, jede in der Multiplicität 1 ergeben. Durch Induction kommt man leicht zu der Form (26). Der Beweis ist dem in § 302, Bd. I gegebenen durchaus analog. Es sei ζ eine Wurzel von $\varphi_n(z) - z = 0$, die zum Exponenten

$$\nu = \frac{n}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\delta^{\alpha_\delta}} \qquad (\delta \leqq \varkappa;\ \alpha_i \leqq \nu_i)$$

gehört; dann wird nicht nur $\varphi_\nu(\zeta) = \zeta$, sondern jedes $\varphi_{\varrho\nu}(\zeta) = \zeta$ befriedigt, wenn ϱ eine ganze Zahl bedeutet. Insbesondere gilt das für

$$\varrho\nu = n;\ \frac{n}{p_1},\ \frac{n}{p_2},\ \cdots\ \frac{n}{p_\delta};\ \frac{n}{p_1p_2},\ \cdots\ \frac{n}{p_{\delta-1}p_\delta};\ \frac{n}{p_1p_2p_3},\ \cdots$$

Es tritt deshalb der Wurzelfactor $(z - \zeta)$ in (26) mit der Multiplicität 1 in den folgenden Factoren des Zählers oder des Nenners

$$[n:1];\ [n:p_1],\ \cdots\ [n:p_\delta];\ [n:p_1p_2],\ \cdots\ [n:p_{\delta-1}p_\delta];\ \cdots$$

auf. Sonach ist das gesammte Eingehen des Factors $(z - \zeta)$ in (26) von der Multiplicität

$$1 - \binom{\delta}{1} + \binom{\delta}{2} - \binom{\delta}{3} + \cdots \pm \binom{\delta}{\delta} = (1-1)^\delta = 0,$$

d. h. der Factor hebt sich überhaupt heraus. Nur wenn $\nu = n$, und also ζ eine primitive Wurzel ist, dann wird dieser Schluss ungültig, δ gewissermassen Null, und man erhält $(z - \zeta)$ einmal im Zähler.

Damit ist gezeigt worden, dass Φ_n eine ganze Function ist, und dass $\Phi_n(z) = 0$ alle und nur die primitiven Wurzeln von $\varphi_n(z) - z = 0$, jede ein einziges Mal liefert. Hierdurch sind wir zu Gleichungen gelangt, wie wir sie in § 489 behandelt haben. Ihre Wurzeln können in das Schema (4) eingeordnet werden. So erhalten wir die Möglichkeit, alle Gleichungs-Polygone herzustellen, für welche φ und n gegeben ist; sie müssen sämmtlich Theiler von (26) sein.

Nach Auflösung einer gewissen Gleichung (5) kann man die Gleichungen n^{ten} Grades herstellen (7), von denen die Elemente je einer Zeile in (4) als Wurzeln abhängen. Hat insbesondere (5) eine rationale Wurzel, so befinden sich die Coefficienten der entsprechenden Gleichung (7) gleichfalls im natürlichen Rationalitätsbereiche, d. h. demjenigen, welcher aus allen rationalen Zahlen besteht. Damit haben wir also eine cyklische Gleichung erlangt und zugleich die charakteristische Bedingung dafür abgeleitet, dass eine solche für eine gewisse gegebene Function $\varphi(z)$ überhaupt besteht. Denn umgekehrt muss (5) eine rationale Wurzel haben, sobald eine solche cyklische Gleichung vorhanden ist.

§ 500. Wir wollen die gegebenen allgemeinen Vorschriften durch zwei Beispiele illustriren. Zunächst sollen alle cyklischen Gleichungen dritten Grades bestimmt werden. Dabei dürfen wir

$$\varphi(z_1) = mz_1^2 + nz_1 + p$$

setzen; da aber nach dem Satze aus § 498 auch $\alpha z_1 + \beta$ die Wurzel einer cyklischen Gleichung ist, so können wir α und β so bestimmen, dass von vornherein das Glied mit z verschwindet, und dass sonach

$$\varphi(z_1) = z^2 + a$$

angenommen werden kann. Hierfür wird

$$(27)\quad \frac{\varphi_3(z) - z}{\varphi(z) - z} = z^6 + z^5 + (3a+1)z^4 + (2a+1)z^3 + (3a^2 + 3a + 1)z^2 \\ + (a^2 + 2a + 1)z + (a^3 + 2a^2 + a + 1) = 0$$

die Gleichung, deren Zerlegung in zwei cubische Gleichungen erstrebt werden muss. Wir verstehen unter z' eine Wurzel von (27) und setzen

$$z' + \varphi(z') + \varphi_2(z') = \vartheta_1(z'),$$
$$z'\varphi(z') + \varphi(z')\varphi_2(z') + \varphi_2(z')z' = \vartheta_2(z'),$$
$$z'\varphi(z')\varphi_2(z') = \vartheta_3(z').$$

Als Werthe dieser Functionen ergeben sich aus der Definition von $\varphi(z)$ und mit Hülfe von (27)

$$\vartheta_1(z') = z'^4 + (2a+1)z'^2 + z' + (a^2 + 2a),$$
$$\vartheta_2(z') = z'^6 + z'^5 + 3az'^4 + (2a+1)z'^3 + (3a^2 + a)z'^2 \\ + (a^2 + 2a)z' + (a^3 + a^2)$$
$$= \frac{\varphi_3(z') - z'}{\varphi(z') - z'} - \vartheta_1(z') + (a-1)$$
$$= -\vartheta_1(z') + (a-1),$$

$$\vartheta_3(z') = z'^7 + 3az'^5 + (3a^2 + a)z'^3 + (a^3 + a^2)z'$$
$$= (z' - 1)\frac{\varphi_3(z') - z'}{\varphi(z') - z'} + a\vartheta_1(z') + (a + 1)$$
$$= a\vartheta_1(z') + (a + 1),$$

so dass die Gleichung

$$(28)\quad z^3 - \vartheta_1(z') \cdot z^2 - (\vartheta_1(z') - (a - 1))z - (a\vartheta_1(z') + a + 1) = 0$$

die Wurzeln z', $\varphi(z')$, $\varphi_2(z')$ besitzt. Bezeichnet man die übrigen drei Wurzeln von (27) mit z'', $\varphi(z'')$, $\varphi_2(z'')$, so erhält man

$$\vartheta_1(z') + \vartheta_1(z'') = \sum_1^6 z_\lambda = -1,$$

$$\vartheta_1(z') \cdot \vartheta_1(z'') = \sum_1^6 z_\lambda z_\mu - \vartheta_2(z') - \vartheta_2(z'')$$
$$= (3a + 1) + \vartheta_1(z') + \vartheta_1(z'') - 2(a - 1)$$
$$= a + 2,$$

und sonach wird

$$(29)\qquad u^2 + u + (a + 2) = 0$$

die Gleichung, deren Wurzeln $\vartheta_1(z')$ und $\vartheta_1(z'')$ sind. Nach dem Schlusse des vorigen Paragraphen müssen wir dieser Gleichung (29) eine rationale Wurzel zu verschaffen suchen. Es ist

$$u = \frac{1}{2}(-1 \pm \sqrt{-4a - 7});$$

demnach entstehen für die allgemeinste Annahme

$$-(4a + 7) = (2\lambda + 1)^2, \quad a = -(\lambda^2 + \lambda + 2)$$

die rationalen Wurzeln

$$u = \frac{1}{2}(-1 \pm 2\lambda \pm 1), \quad \text{d. h.} \quad u_1 = \lambda, \quad u_2 = -\lambda - 1,$$

und wir können setzen

$$\vartheta_1(z') = \lambda, \quad \vartheta_1(z'') = -(\lambda + 1).$$

Dadurch entstehen aus (28) die beiden cyklischen Gleichungen

$$(30)\quad \begin{aligned} &z^3 - \lambda z^2 - (\lambda^2 + 2\lambda + 3)z + (\lambda^3 + 2\lambda^2 + 3\lambda + 1) = 0, \\ &z^3 + (\lambda + 1)z^2 - (\lambda^2 + 2)z - (\lambda^3 + \lambda^2 + 2\lambda + 1) = 0. \end{aligned}$$

Das Product der linken Seiten ergiebt (27), wenn $\lambda^2 + \lambda + 2 = -a$ gesetzt wird. Uebrigens sind die beiden Gleichungen (30) nicht wesentlich von einander verschieden; denn durch $\lambda = -(\lambda_1 + 1)$ geht die Form $(\lambda^2 + \lambda + 2)$ in $(\lambda_1^2 + \lambda_1 + 2)$, und die erste der Gleichungen (30)

in die zweite über. Wir können uns daher auf die erste der beiden beschränken. Nehmen wir noch, um die zweite Potenz der Unbekannten zu beseitigen, $\lambda = \frac{3\mu}{2}$, $z = \zeta + \frac{\mu}{2}$, so entsteht

$$\zeta^3 - 3(\mu^2 + \mu + 1)\zeta + (\mu^2 + \mu + 1)(2\mu + 1) = 0 \tag{31}$$

mit den Wurzelrelationen

$$\begin{aligned} \zeta_2 &= \varphi(\zeta_1) = \zeta_1^2 + \mu\zeta_1 - 2(\mu^2 + \mu + 1), \\ \zeta_3 &= \varphi_2(\zeta_1) = -\zeta_1^2 - (\mu + 1)\zeta_1 + 2(\mu^2 + \mu + 1). \end{aligned}$$

Auf die Form (31) kann also jede cyklische Gleichung dritten Grades reducirt werden.

Ist eine solche Gleichung (31) vorgelegt, so fordert die nach unserer Methode durchzuführende Auflösung vor Allem die Bildung der Lagrange'schen Resolvente $(\zeta_1 + \zeta_2\omega + \zeta_3\omega^2)^3$. Zur Berechnung dienen die Formeln

$$\begin{aligned} \zeta_1 + \zeta_2 + \zeta_3 &= 0, \\ \zeta_1^2 + \zeta_2^2 + \zeta_3^2 &= 6(\mu^2 + \mu + 1), \\ \zeta_1\zeta_2 + \zeta_2\zeta_3 + \zeta_3\zeta_1 &= -3(\mu^2 + \mu + 1), \\ \zeta_1^3 + \zeta_2^3 + \zeta_3^3 &= -3(2\mu + 1)(\mu^2 + \mu + 1), \\ \zeta_1^2\zeta_2 + \zeta_2^2\zeta_3 + \zeta_3^2\zeta_1 &= 3(\mu + 2)(\mu^2 + \mu + 1), \\ \zeta_1\zeta_2^2 + \zeta_2\zeta_3^2 + \zeta_3\zeta_1^2 &= 3(\mu - 1)(\mu^2 + \mu + 1), \\ \zeta_1\zeta_2\zeta_3 &= -(2\mu + 1)(\mu^2 + \mu + 1), \end{aligned}$$

welche sich leicht durch die Relationen

$$\begin{aligned} \zeta_2^2 &= -(\mu + 1)\zeta_1^2 - (\mu^2 + \mu + 1)\zeta_1 + 2(\mu + 2)(\mu^2 + \mu + 1), \\ \zeta_3^2 &= \mu\zeta_1^2 + (\mu^2 + \mu + 1)\zeta_1 - 2(\mu - 1)(\mu^2 + \mu + 1) \end{aligned}$$

bilden lassen. Mit ihrer Hülfe erhält man

$$(\zeta_1 + \zeta_2\omega + \zeta_3\omega^2)^3 = 27(\omega - \mu)(\mu^2 + \mu + 1),$$

und also

$$\begin{aligned} \zeta_1 + \zeta_2 + \zeta_3 &= 0, \\ \zeta_1 + \omega\zeta_2 + \omega^2\zeta_3 &= 3\sqrt[3]{\omega - \mu}\,\sqrt[3]{\mu^2 + \mu + 1}, \\ \zeta_1 + \omega^2\zeta_2 + \omega\zeta_3 &= 3\sqrt[3]{\omega^2 - \mu}\,\sqrt[3]{\mu^2 + \mu + 1}. \end{aligned}$$

Daher wird die Lösung der Gleichung (31) durch die Formeln geliefert

$$\begin{aligned} \zeta_1 &= \sqrt[3]{\omega - \mu}\,\sqrt[3]{\mu^2 + \mu + 1} + \sqrt[3]{\omega^2 + \mu}\,\sqrt[3]{\mu^2 + \mu + 1} \\ &= \sqrt[3]{(\omega - \mu)^2(\omega^2 - \mu)} \quad + \frac{\mu^2 + \mu + 1}{\sqrt[3]{(\omega - \mu)^2(\omega^2 - \mu)}}, \end{aligned}$$

$$\zeta_2 = \omega^2 \sqrt[3]{(\omega-\mu)^2(\omega^2-\mu)} + \frac{\mu^2+\mu+1}{\omega^2\sqrt[3]{(\omega-\mu)^2(\omega^2-\mu)}},$$

$$\zeta_3 = \omega \sqrt[3]{(\omega-\mu)^2(\omega^2-\mu)} + \frac{\mu^2+\mu+1}{\omega\sqrt[3]{(\omega-\mu)^2(\omega^2-\mu)}}.$$

Nach den Bemerkungen zu Anfang des § 498 wissen wir jetzt, dass die Discriminante von (31) im natürlichen Rationalitätsbereiche ein vollständiges Quadrat sein muss; in der That wird auch (vgl. § 283, Bd. I) dieser Ausdruck gleich

$$108(\mu^2+\mu+1)^3 - 27(\mu^2+\mu+1)^2(2\mu+1)^2 = 9^2(\mu^2+\mu+1)^2.$$

Bemerkenswerth ist, was aus den beiden Gleichungen (30) hervorgeht: dass jeder cyklischen Gleichung dritten Grades eine andere zugeordnet ist, welche dieselben Wurzelrelationen aufweist, wie jene.

Aus (31) kann man die allgemeinste cyklische Gleichung dritten Grades von der Form

$$u^3 - 3Au + B = 0$$

herleiten, wenn man auf (31) die allgemeinste Tschirnhausen-Transformation anwendet, für welche das Glied mit der zweiten Potenz der Unbekannten verschwindet. Diese ist, wie eine leichte Rechnung ergiebt, bei $\mu^2+\mu+1=a$, von der Form

$$\zeta = \alpha u^2 + \beta u - 2a\alpha, \tag{32}$$

und man erhält nach Unterdrückung des Factors $(3a\alpha^2\beta - b\alpha^3 - \beta^3)$,

$$\begin{aligned}\zeta^3 &- 3(a^2\alpha^2 + a\beta^2 - b\alpha\beta)\zeta \\ &+ (2a^3\alpha^3 - 6a^2\alpha\beta^2 + 3ab\alpha^2\beta + b\beta^3 - b^2\alpha^3) = 0 \\ &(a = \mu^2+\mu+1,\quad b = (\mu^2+\mu+1)(2\mu+1)).\end{aligned} \tag{33}$$

Die erhaltenen Coefficienten geben die allgemeinste Lösung der Aufgabe, A und B so zu bestimmen, dass $(4A^3 - B^2)$ das Dreifache eines vollständigen Quadrates wird.

§ 501. Wir fragen weiter nach denjenigen Gleichungen vierten Grades, deren Wurzeln durch

$$z',\quad \varphi(z'),\quad \varphi_2(z'),\quad \varphi_3(z')$$

dargestellt werden können, wobei aber, um die Rechnung nicht zu complicirt werden zu lassen, einfach

$$\varphi(z) = z^2 + a$$

angenommen werden soll. Hierfür findet man

$$\frac{\varphi_4(z)-z}{\varphi_2(z)-z} \equiv z^{12}+6az^{10}+z^9+(15a^2+3a)z^8+4az^7+(20a^3+12a^2+1)z^6$$
$$+(6a^2+2a)z^5+(15a^4+18a^3+3a^2+4a)z^4$$
$$+(4a^3+4a^2+1)z^3+(6a^5+12a^4+6a^3+5a^2+a)z^2$$
$$+(a^4+2a^3+a^2+2a)z$$
$$+(a^6+3a^5+3a^4+3a^3+2a^2+1)=0,$$

so dass diese Gleichung die zwölf Wurzeln

$$z^{(i)}, \quad \varphi(z^{(i)}), \quad \varphi_2(z^{(i)}), \quad \varphi_3(z^{(i)}) \qquad (i=1,2,3)$$

besitzt. Die elementaren symmetrischen Functionen der vier zu gleichem i gehörigen Wurzeln setzen wir

$$\vartheta_1(z^{(i)}), \quad \vartheta_2(z^{(i)}), \quad \vartheta_3(z^{(i)}), \quad \vartheta_4(z^{(i)})$$

und wissen dann, dass die drei Grössen

$$\vartheta_1(z'), \quad \vartheta_1(z''), \quad \vartheta_1(z''')$$

einer Gleichung dritten Grades mit rationalen Coefficienten genügen. Man findet für sie auf dem im vorigen Paragraphen eingeschlagenen Wege

$$u^3+(4a+3)u+4=0. \tag{34}$$

Mit Hülfe von (34) kann man die dritte und alle höheren Potenzen von $\vartheta_1(z')$ durch niedere ausdrücken; so erhält man

$$\vartheta_2(z') = \frac{1}{2}[\vartheta_1(z')^2-\vartheta_1(z')+4a],$$
$$\vartheta_3(z') = -\frac{1}{2}[\vartheta_1(z')^2-(2a-1)\vartheta_1(z')+2],$$
$$\vartheta_4(z') = \frac{1}{2}[a\vartheta_1(z')^2+a\vartheta_1(z')+2a^2+2a+2].$$

Demnach genügen die Grössen z', $\varphi(z')$, $\varphi_2(z')$, $\varphi_3(z')$ der Gleichung

$$\begin{aligned} u^4-\vartheta_1(z')\cdot u^3+\frac{1}{2}[\vartheta_1(z')^2-\vartheta_1(z')+4a]u^2 \\ +\frac{1}{2}[\vartheta_1(z')^2-(2a-1)\vartheta_1(z')+2]u \\ +\frac{1}{2}[a\vartheta_1(z')^2+a\vartheta_1(z')+2a^2+2a+2]=0. \end{aligned} \tag{35}$$

Hat (34) eine rationale Wurzel $\vartheta_1(z')$, dann ist (35) eine cyklische Gleichung. Wir setzen demnach das Polynom von (34)

$$u^3+(4a+3)u+4=(u-\varkappa)(u^2+\varkappa u+\lambda)$$

und erhalten für diese Zerlegungsmöglichkeit

$$\varkappa\lambda = -4, \quad \lambda - \varkappa^2 = 4a + 3;$$

$$a = -\frac{\varkappa^3 + 3\varkappa + 4}{4\varkappa};$$

$$u = \vartheta_1(z') = \varkappa.$$

Folglich ist die gesuchte allgemeinste cyklische Gleichung

$$(35^a) \quad u^4 - \varkappa u^3 - \frac{\varkappa^2 + 3\varkappa + 4}{2\varkappa} u^2 + \frac{\varkappa^3 + 2\varkappa^2 + 5\varkappa + 8}{4} u + \frac{\varkappa^5 - 2\varkappa^4 + 4\varkappa^3 - 2\varkappa^2 + 11\varkappa + 4}{16\varkappa} = 0$$

mit der Wurzelrelation

$$u_2 = \varphi(u_1) = u_1^2 - \frac{\varkappa^3 + 3\varkappa + 4}{4\varkappa}.$$

§ 502. Häufig erscheint eine Gleichung, von welcher eine Reihe unbekannter Grössen $z_1, z_2, \cdots z_n$ als Wurzeln abhängt, als analytischer Ausdruck eines Problems, aus dem sich der Natur der Fragestellung gemäss von vornherein erkennen lässt, dass für $z_1, z_2, \cdots z_n$ die charakteristischen Beziehungen für cyklische Gleichungen $z_2 = \varphi(z_1)$, $z_3 = \varphi(z_2), \cdots$ herrschen; und häufig wird gleichzeitig die Function φ selbst dabei gegeben sein. Hier macht es dann keine Mühe, die auseinandergesetzten Methoden der Lösung in Anwendung zu bringen. Anders ist es dagegen, wenn eine fertige Gleichung vorgelegt und gefragt wird, ob sie zu den cyklischen Gleichungen gehört, und wie die Function φ bestimmt werden kann, falls eine solche besteht. Wir wollen die aufgeworfene Frage, soweit es hier möglich ist, kurz behandeln.

Auf die zu prüfende Gleichung $f(z) = 0$ wenden wir eine Tschirnhausen'sche Transformation mit noch unbestimmten Coefficienten an

$$\zeta = \alpha_1 z^{n-1} + \beta_1 z^{n-2} + \cdots + \delta_1;$$

aus ihr folge, nach den nöthigen Reductionen durch $f = 0$,

$$\zeta^2 = \alpha_2 z^{n-1} + \beta_2 z^{n-2} + \cdots + \delta_2,$$
$$\zeta^3 = \alpha_3 z^{n-1} + \beta_3 z^{n-2} + \cdots + \delta_3,$$
$$\cdots\cdots\cdots\cdots\cdots$$

Durch Elimination von $z^{n-1}, \cdots z$ entstehe $F(\zeta) = 0$, welches wie f vom Grade n wird. Ist nun $f(z) = 0$ cyklisch, so müssen $\alpha_1, \beta_1, \cdots \delta_1$ sich so wählen lassen, dass $F(\zeta)$ bis auf einen constanten Factor mit $f(z)$ übereinstimmt. Setzt man die hierzu nöthigen Gleichungen an, dann ist das Bestehen eines im Rationalitätsbereiche enthaltenen Lösungssystems charakteristisch dafür, dass f cyklisch sei. Die gefundene Tschirnhausen'sche Transformationsformel liefert gleichzeitig die Form der Function $\varphi(z)$.

Wir wollen diese, in der Theorie sehr einfache, in der Ausführung recht umständliche Methode auf ein übersichtliches Beispiel anwenden.

Wir nehmen als zu prüfende Gleichung

$$f(z) \equiv z^3 - 3az + b = 0$$

und fragen also, wann diese cyklisch werden wird.

Dafür erhält man mit Hülfe der Substitution (32), welche offenbar nothwendig ist, und durch welche die Rechnung abgekürzt wird,

$$\zeta = \alpha z^2 + \beta z - 2a\alpha,$$

$$\zeta^2 = (\beta^2 - a\alpha^2)z^2 + (2a\alpha\beta - \alpha^2 b)z + (4a^2\alpha^2 - 2b\alpha\beta),$$

$$\zeta^3 = (3a^2\alpha^3 + 3a\alpha\beta^2 - 3b\alpha^2\beta)z^2 + (3a^2\alpha^2\beta + 3a\beta^3 - 3b\alpha\beta^2)z$$
$$+ (-8a^3\alpha^3 + 3ab\alpha^2\beta - b\beta^3 + b^2\alpha^3).$$

Aus der transformirten Function lässt sich $(3a\alpha^2\beta - \alpha^3 b - \beta^3)$ als gemeinsamer Factor aller Coefficienten heraussetzen. Die zurückbleibende Function lautet

$$F(\zeta) = \zeta^3 - 3(a^2\alpha^2 + a\beta^2 - b\alpha\beta)\zeta$$
$$+ (2a^3\alpha^3 - 6a^2\alpha\beta^2 + 3ab\alpha^2\beta + b\beta^3 - b^2\alpha^3).$$

Hier sind nun α und β so zu bestimmen, dass $F(z)$ mit $f(z)$ identisch wird; d. h. damit $f(z) = 0$ cyklisch sei, muss das System der beiden Gleichungen

$$a\beta^2 - b\alpha\beta + (a^2\alpha^2 - a) = 0,$$

$$b\beta^3 - 6a^2\alpha\beta^2 + 3ab\alpha^2\beta + (2a^3\alpha^3 - b^2\alpha^3 - b) = 0$$

eine rationale Wurzel (α, β) besitzen. Die Eliminante der Gleichungen wird

$$(36)\quad \alpha(4a^3 - b^2)[(4a^3 - b^2)\alpha^2 - 3a^2][(4a^3 - b^2)\alpha^3 - 3a^2\alpha - b].$$

Das zu α gehörige β entnimmt man dann der Gleichung

$$\beta[b(4a^3 - b^2)\alpha^2 - a^2 b] = 2a^2(4a^3 - b^2)\alpha^3 + a(b^2 - 6a^3)\alpha - a^2 b.$$

Hier führt der erste Factor von (36) auf $\beta = 1$ und somit zu dem banalen Resultate $\zeta = z$; das ergiebt keine cyklische Gleichung.

Der zweite Factor ist die Discriminante der vorgelegten Gleichung; er verschwindet für $a = q^2$, $b = 2q^3$, und das giebt

$$f(z) \equiv z^3 - 3q^2 z + 2q^3 = (z + 2q)(z - q)^2,$$

$$F(\zeta) \equiv \zeta^3 - 3(q^2\alpha - q\beta)^2\zeta - 2(q^2\alpha - q\beta)^3.$$

Damit $F(z) \equiv f(z)$ werde, reicht es aus, bei beliebigem q

$$\beta = q\alpha + 1$$

zu setzen. Man hat also für jedes

$$\zeta = \alpha z^2 + (q\alpha + 1)z - 2q^2\alpha = \alpha(z - q)(z + 2q) + z$$

die gewünschte Identität. Dass unendlich viele Lösungen auftreten, ist durch das identische Verschwinden der Eliminante bedingt.

Zur Behandlung des Factors $[(4a^3 - b^2)\alpha^2 - 3a^2]$ führen wir

$$4a^3 - b^2 = 3\Delta^2$$

ein; dadurch wird

$$\alpha = \frac{a}{\Delta}, \quad \beta = \frac{b - \Delta}{2\Delta},$$

und es handelt sich also nur noch darum, a und b so zu bestimmen, dass die Grösse Δ dem Rationalitätsbereiche angehört. Dies wird im natürlichen Rationalitätsbereiche, wie wir in § 500 am Schlusse gesehen haben, durch die Annahme

$$a = \mu^2 + \mu + 1, \quad b = (\mu^2 + \mu + 1)(2\mu + 1)$$

geleistet. Hierbei wird $\Delta = a$, und

$$\zeta = \varphi(z) = \quad z^2 + \mu z \qquad - 2(\mu^2 + \mu + 1),$$
$$\varphi(\zeta) = \varphi_2(z) = -z^2 - (\mu + 1)z + 2(\mu^2 + \mu + 1);$$

es entsteht demnach $\varphi_2(z)$ aus $\varphi(z)$, wenn man Δ durch $-\Delta$ ersetzt. —

Es wäre endlich noch der Factor

$$(4a^3 - b^2)\alpha^3 - 3a^2\alpha - b$$

zu untersuchen. Darauf wollen wir nicht direct eingehen, weil dies zu complicirten Rechnungen führt, sondern die Frage durch die Bemerkung entscheiden, dass für jedes hierher gehörige

$$\zeta = \alpha z^2 + \beta z - 2a\alpha$$

$\varphi(\zeta) = \varphi_2(z) = z$ wird. In diesem Falle ist nämlich

$$(4a^3 - b^2)\alpha^3 - 3a^2\alpha - b = 0,$$

$$\beta = \frac{a(a + b\alpha)}{(4a^3 - b^2)\alpha^2 - a^2},$$

$$\varphi(\zeta) = (\alpha\beta^2 - a\alpha^3 + \alpha\beta)z^2 + (2a\alpha^2\beta - b\alpha^3 + \beta^2)z$$
$$+ (4a^2\alpha^3 - 2a\alpha - 2b^2\alpha\beta - 2a\alpha\beta).$$

Mit Hülfe der beiden ersten dieser Gleichungen verwandelt sich der letzte Ausdruck nun in $\varphi(\zeta) = z$. Da aber die drei Wurzeln von $f = 0$ durch z, $\varphi(z)$, $\varphi_2(z)$ dargestellt werden, so kann nicht $\varphi_2(z) = z$ sein, ohne dass sämmtliche Wurzeln einander gleich werden. —

Wir bemerken noch, dass der Uebergang von $f(z)$ zu $F(\zeta)$ am einfachsten durch die zu

$$f(z) = 0 \quad \text{und} \quad \alpha_1 z^{n-1} + \beta_1 z^{n-2} + \cdots + (\delta_1 - \zeta) = 0$$

gehörige Eliminationsdeterminante gemacht wird.

Fünfzigste Vorlesung.

Die Abel'schen Gleichungen.

§ 503. Nach den Darlegungen der letzten Vorlesung wird man zu der allgemeineren Frage nach denjenigen Gleichungen geführt, bei welchen alle Wurzeln durch eine unter ihnen rational darstellbar sind. Solchen Gleichungen werden wir später unsere Aufmerksamkeit zuzuwenden haben; hier erwähnen wir nur, dass diese Gleichungen im Allgemeinen nicht algebraisch auflösbar sind. Dagegen hat Abel in seiner schon erwähnten Abhandlung eine Classe von Gleichungen speciellerer Art angegeben, bei denen durch Hinzufügung einer neuen Bedingung zur rationalen Darstellbarkeit aller Wurzeln durch eine unter ihnen die algebraische Auflösbarkeit herbeigeführt wird. Abel stellt folgenden Lehrsatz auf*): Es sei $f(z)=0$ eine algebraische Gleichung m^{ten} Grades, deren Wurzeln sämmtlich durch eine unter ihnen, z', rational ausdrückbar sind. Sind in dieser Darstellung $\varphi(z')$, $\chi(z')$ zwei willkürliche Wurzeln, und ist für sie $\varphi(\chi(z'))=\chi(\varphi(z'))$, so ist die Gleichung algebraisch auflösbar.

Solche Gleichungen wollen wir Abel'sche Gleichungen nennen. Es ist ersichtlich, dass die cyklischen Gleichungen als Abel'sche Gleichungen einfachster Art aufgefasst werden können; vergleiche dazu im Folgenden die Darlegungen aus § 517, in denen eine eingehendere Classification der Abel'schen Gleichungen gegeben werden soll.

§ 504. Unsere Gleichungen stehen unter den in § 489 behandelten, sobald wir auch hier die Irreductibilität voraussetzen. Das aber können wir unbedenklich thun, da ja, wenn $f_1(z)$ ein irreductibler Factor von $f(z)$ ist, für die Wurzeln von $f_1=0$ die obigen Voraussetzungen gleichfalls gelten, und da andererseits mit der Kenntniss von z' alle anderen Wurzeln bekannt werden. Man kann sich somit auf einen und zwar auf denjenigen irreductiblen Factor von f beschränken, bei dem $(z-z')$ als Wurzelfactor vorkommt.

Demnach können wir unsere früheren Resultate verwerthen und die m Wurzeln von $f=0$ in das Schema

*) Oeuvres, éd. Sylow et Lie; 1, p. 479.

$$
(1)\quad
\begin{array}{llllll}
z', & \varphi(z'), & \varphi_2(z'), & \cdots & \varphi_{n-1}(z'), & (\varphi_n(z') = z') \\
z'', & \varphi(z''), & \varphi_2(z''), & \cdots & \varphi_{n-1}(z''), & (\varphi_n(z'') = z'') \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
z^{(\nu)}, & \varphi(z^{(\nu)}), & \varphi_2(z^{(\nu)}), & \cdots & \varphi_{n-1}(z^{(\nu)}), & (\varphi_n(z^{(\nu)}) = z^{(\nu)})
\end{array}
$$
$$(n \cdot \nu = m)$$

einordnen. Ist $\nu = 1$, dann befinden wir uns in dem Falle von cyklischen Gleichungen. Wir setzen daher jetzt $\nu > 1$ voraus und bilden die Werthe einer allgemeinen noch unbestimmten symmetrischen Function S

$$
(2)\quad
\begin{array}{l}
y' = S(z', \varphi(z'), \varphi_2(z'), \cdots \varphi_{n-1}(z')) = F(z'), \\
y'' = S(z'', \varphi(z''), \varphi_2(z''), \cdots \varphi_{n-1}(z'')) = F(z''), \\
\cdots\cdots\cdots\cdots\cdots\cdots \\
y^{(\nu)} = S(z^{(\nu)}, \varphi(z^{(\nu)}), \varphi_2(z^{(\nu)}), \cdots \varphi_{n-1}(z^{(\nu)})) = F(z^{(\nu)}),
\end{array}
$$

wobei wir, wie dies auch früher geschehen ist, Sorge dafür tragen wollen, dass alle diese ν Werthe des S verschieden von einander ausfallen.

Nun wissen wir (§ 491), dass die Gleichung

$$(3)\qquad h_\alpha(z) \equiv (z - z^{(\alpha)})\,(z - \varphi(z^{(\alpha)})) \cdots (z - \varphi_{n-1}(z^{(\alpha)})) = 0,$$
$$(\alpha = 1, 2, \cdots \nu)$$

welche $z^{(\alpha)}, \varphi(z^{(\alpha)}), \cdots$ als Wurzeln liefert, eine cyklische Gleichung und deshalb durch Verwendung von Wurzelausziehungen auflösbar ist. Wir wissen ferner, dass ihre Coefficienten als symmetrische Functionen von $z^{(\alpha)}, \varphi(z^{(\alpha)}), \cdots$ rational durch jede andere symmetrische Function derselben Grössen ausdrückbar sind, sobald diese für $\alpha = 1, 2, \cdots \nu$ verschiedene Werthe annimmt (§ 490); dass wir also gemäss unserer Vorbereitungen die Coefficienten von $h_\alpha(z)$ rational durch $y^{(\alpha)}$ ausdrücken und somit statt $h_\alpha(z)$ schreiben dürfen

$$(4)\quad h(z; y^{(\alpha)}) \equiv z^n - \gamma_1(y^{(\alpha)}) \cdot z^{n-1} + \gamma_2(y^{(\alpha)}) \cdot z^{n-2} - \cdots \pm \gamma_n(y^{(\alpha)}) = 0.$$

Die Auflösung der Abel'schen Gleichung mit den Wurzeln (1) ist demnach abhängig von derjenigen einer Gleichung mit den Wurzeln (2), wobei die symmetrische Function S, abgesehen von der oben erwähnten Einschränkung, beliebig angenommen werden kann.

Wir setzen nun die irreductible Gleichung an

$$(5)\qquad g(y) \equiv (y - y')\,(y - y'') \cdots (y - y^{(\nu)}) = 0$$

und erkennen, dass die Coefficienten von g rational durch die Coefficienten der vorgelegten Abel'schen Gleichung darstellbar sind (§ 490). Schreiben wir also

$$(6) \qquad g(y) \equiv y^\nu - d_1 y^{\nu-1} + d_2 y^{\nu-2} - \cdots \pm d_\nu = 0,$$

so sind die d rational bekannt. Es hängt also Alles von der Natur der Gleichung (6) ab. Wir werden zeigen, dass sie wiederum eine Abel'sche Gleichung ist.

§ 505. Es ist den Voraussetzungen gemäss auch z'' eine Function von z', also etwa $z'' = \chi(z')$; ebenso sind die beiden Functionalzeichen φ und χ, auf z' angewendet, mit einander vertauschbar, d. h. $\chi(\varphi(z')) = \varphi(\chi(z'))$; somit wird $\chi(\varphi_2(z')) = \varphi_2(\chi(z')), \cdots$, und daher

$$\begin{aligned} y'' = F(z'') &= S(\chi(z'),\ \varphi(\chi(z')),\ \varphi_2(\chi(z')), \cdots) \\ &= S(\chi(z'),\ \chi(\varphi(z')),\ \chi(\varphi_2(z')), \cdots) \\ &= S_1(z',\ \varphi(z'),\ \varphi_2(z'), \cdots), \end{aligned}$$

wo S_1 auch eine symmetrische Function ist. Demnach wird, falls λ eine passend gewählte rationale Function bedeutet,

$$(7) \qquad y'' = F(\chi(z')) = \lambda(y').$$

Ebenso folgt, wenn wir etwa $z''' = \varpi(z')$ annehmen, für eine passend gewählte Function μ

$$(7^a) \qquad y''' = F(\varpi(z')) = \mu(y').$$

Nun ergiebt sich aus (2), dass, wenn man an die Stelle von z' setzt z'' oder z''', dann y' in y'' bezw. in y''' übergeht. Daher zeigen (7) und (7ª) die Richtigkeit der Gleichungen

$$\begin{aligned} \lambda(y''') &= F(\chi(z''')) \quad \text{d. h.} \quad \lambda(\mu(y')) = F[\chi(\varpi(z'))]; \\ \mu(y'') &= F(\varpi(z'')) \quad \text{d. h.} \quad \mu(\lambda(y')) = F[\varpi(\chi(z'))]. \end{aligned}$$

Der Annahme nach ist $\chi\varpi(z') = \varpi\chi(z')$; demnach hat man endlich

$$(8) \qquad \lambda(\mu(y')) = \mu(\lambda(y')).$$

Die Gleichungen (7) und (7ª) liefern den Nachweis dafür, dass jede Wurzel von (6) eine rationale Function von y' ist, und (8) zeigt, dass die hierbei auftretenden Functionaloperationen auf y' angewendet mit einander vertauschbar seien. Folglich sind alle Voraussetzungen dafür erfüllt, dass auch (6) eine Abel'sche Gleichung ist. Auf sie kann wieder dieselbe Schlussweise angewendet werden.

Hiermit ist dann zugleich die Auflösbarkeit der Abel'schen Gleichung $f(z) = 0$ dargethan. Denn $g(y) = 0$ ist entweder cyklisch, und dann ist die Frage bereits erledigt; oder wenn dies nicht so ist, dann können wir auf $g = 0$ dieselben Schlüsse anwenden, wie soeben, und führen ihre Lösung dadurch auf die einer Abel'schen Gleichung eines Grades zurück, der ein echter Theiler von n ist. Die Methode führt daher stets auf eine Reihe cyklischer Gleichungen. Nach unseren Ab-

leitungen ist es ersichtlich, dass das Product der Gradzahlen dieser Gleichungen m sein wird. Nehmen wir hierzu noch die Resultate aus § 491, so erkennen wir: Die Auflösung einer irreductiblen Abel'schen Gleichung m^{ten} Grades kann durch diejenige einer Reihe cyklischer Gleichungen von Primzahlgraden geliefert werden, bei denen das Product der Grade gleich m ist.

§ 506. Als Beispiel für Abel'sche Gleichungen behandeln wir diejenigen, von denen die Theilung des Kreises in n gleiche Theile abhängt, indem wir dabei $\cos\frac{2\pi}{n}$ als Unbekannte ansehen. Die Wurzeln der Gleichung sind $\cos\frac{2\lambda\pi}{n}$ für $\lambda = 1, 2, \cdots n$; die Form der Gleichung können wir aus § 308, Bd. I entnehmen. Wenn wir daselbst für c eintragen $\frac{1}{2}u$ und nach Potenzen von u ordnen, so ergiebt sich, gleichgültig ob n gerade oder ungerade ist, die Gestalt

$$(9)\quad \begin{aligned} &u^n - \frac{n}{1}u^{n-2} + \frac{n(n-3)}{2!}u^{n-4} - \frac{n(n-4)(n-5)}{3!}u^{n-6} \\ &\qquad + \frac{n(n-5)(n-6)(n-7)}{4!}u^{n-8} - \cdots = 2\cos n\alpha. \end{aligned}$$

Hier ist nun $n\alpha = 2\pi$ zu setzen, also $2\cos n\alpha = 2$, dann erhält man die Gleichung

$$(10)\quad u^n - \frac{n}{1}u^{n-2} + \frac{n(n-3)}{2!}u^{n-4} - \cdots = +2 \quad \text{oder} \quad \Phi_n(u) = 0,$$

wobei die linke Seite der ersten Form für ungerade $n = 2m+1$ mit dem Gliede $(-1)^m(2m+1)u$, dagegen für gerade $n = 2m$ mit $(-1)^m \cdot 2$ schliesst.

Wir wollen jetzt $2\cos\frac{2\lambda\pi}{n} = u_\lambda$ setzen, so dass (10) als Wurzeln die Grössen $u_1, u_2, \cdots u_n$ besitzt. Aus den Lehren der Goniometrie ist bekannt, dass u_λ eine ganze, ganzzahlige Function von u_1 ist, also etwa

$$u_\lambda = 2\cos\frac{2\lambda\pi}{n} = \Theta_\lambda(u_1) = \Theta_\lambda\left(2\cos\frac{2\pi}{n}\right),$$

$$u_\mu = 2\cos\frac{2\mu\pi}{n} = \Theta_\mu(u_1) = \Theta_\mu\left(2\cos\frac{2\pi}{n}\right).$$

Hieraus ergeben sich die beiden Beziehungen

$$\Theta_\lambda(\Theta_\mu(u_1)) = \Theta_\lambda(u_\mu) = 2\cos\frac{2\lambda\mu\pi}{n},$$

$$\Theta_\mu(\Theta_\lambda(u_1)) = \Theta_\mu(u_\lambda) = 2\cos\frac{2\lambda\mu\pi}{n},$$

und daraus

$$\Theta_\mu(\Theta_\lambda(u_1)) = \Theta_\lambda(\Theta_\mu(u_1)),$$

so dass wir es also wirklich mit einer Abel'schen Gleichung zu thun haben. Diese Gleichung $\Phi_n(u) = 0$ ist nicht irreductibel; sie hat ja stets $u = 2$ zur Wurzel, und wenn n gerade ist, auch $u = -2$. Ferner erkennt man, dass höchstens diejenigen Wurzeln $2\cos\frac{2\lambda\pi}{n}$ einer irreductiblen Gleichung angehören und nicht schon durch ein $\Phi_m = 0$ mit niedrigerem Index m geliefert werden können, bei denen λ relativ prim zu n und kleiner als n ist. Man überzeugt sich weiter leicht, dass das Polynom $\Phi_n(u)$ abgesehen von dem Factor $(u-2)$ bei ungeradem, und (u^2-4) bei geradem n ein Quadrat wird; ebenso, wegen (9), dass die Zerlegung

$$\Phi_{2m}(u) = \Phi_m(u)[\Phi_m(u) + 4]$$

gilt.

Nehmen wir z. B. $n = 48$, so folgt hiernach

$$\begin{aligned} \Phi_{48}(u) &= \Phi_{24}(u)\,[\Phi_{24}(u) + 4], \\ \Phi_{24}(u) + 4 &= [\Phi_8(u) + 4]^2 (u^8 - 8u^6 + 20u^4 - 16u^2 + 1)^2, \end{aligned}$$

und die Wurzelwerthe der letzten Klammer sind

$$u_\lambda = 2\cos\frac{2\lambda\pi}{48} \quad \text{für} \quad \lambda = 1, 5, 7, 11, 13, 17, 19, 23.$$

Hier gelten die goniometrischen Beziehungen

$$\begin{aligned} u_{11} &= u_1^{11} - 11u_1^9 + 44u_1^7 - 77u_1^5 + 55u_1^3 - 11u_1 \\ &= -u_1^2 + 4, \\ u_5 &= u_1^5 - 5u_1^3 + 5u_1, \end{aligned}$$

wobei die Reduction des Werthes von u_{11} vermittels der Gleichung

$$u^8 - 8u^6 + 20u^4 - 16u^2 + 1 = 0$$

vor sich gegangen ist. Setzt man $u^2 = v$; $u_\lambda^2 = v_\lambda$, so entsteht hieraus für die neue Unbekannte v eine Gleichung

$$v^4 - 8v^3 + 20v^2 - 16v + 1 = 0 \tag{11}$$

mit den Wurzeln

$$\begin{aligned} &v_1; \quad v_1' = -v_1 + 4, \\ &v_2 = -v_1^3 + 6v_1^2 - 8v_1 + 2; \quad v_2' = v_1^3 - 6v_1^2 + 8v_1 + 2. \end{aligned} \tag{12}$$

Dies sind die entscheidenden Wurzelbeziehungen für die Abel'sche Gleichung (11). Setzt man $S(t, t') = t + t'$, so wird

$$\begin{aligned} S(v_1, v_1') + S(v_2, v_2') &= 8, \\ S(v_1, v_1') \cdot S(v_2, v_2') &= 16; \\ S^2 - 8S + 16 &= 0, \\ S &= 4. \end{aligned}$$

Hier tritt daher der früher vorgesehene und stets ausgeschlossene Fall ein, dass S nur einen Werth besitzt. Wir können somit aus dem gewählten $S(v_1, v_1')$ den Werth von $v_1 \cdot v_1'$ nicht bestimmen und setzen, um ihn zu erlangen, $S_1(t, t') = t \cdot t'$. Dann finden wir für diese symmetrische Function

$$S_1(v_1, v_1') = -v_1^2 + 4v_1,$$

$$S_1(v_2, v_2') = \quad 2^2 - (v_1^3 - 6v_1^2 + 8v_1)^2 = v_1^2 - 4v_1 + 4;$$

$$S_1(v_1, v_1') + S_1(v_2, v_2') = 4, \quad S_1(v_1, v_1') \cdot S_1(v_2, v_2') = 1;$$

$$S_1^2 - 4S_1 + 1 = 0,$$

$$S_1 = 2 \pm \sqrt{3}.$$

Daraus sehen wir, dass die Wurzeln von (11) durch die Gleichungen

$$v^2 - 4v + 2 \pm \sqrt{3} = 0$$

gegeben werden, d. h. dass

$$v^4 - 8v^3 + 20v^2 - 16v + 1$$
$$= (v^2 - 4v + 2 + \sqrt{3})(v^2 - 4v + 2 - \sqrt{3})$$

wird. Der grösste Wurzelwerth wird durch die Combination der positiven Vorzeichen der Quadratwurzeln bestimmt

$$v_1 = 2 + \sqrt{2 + \sqrt{3}} = 3,931852\cdots;$$

aus diesem ergiebt sich dann für das entsprechende u

$$\frac{u_1}{2} = \cos\frac{2\pi}{48} = 0,9914449\cdots,$$

und damit die verlangte Theilung des Kreises in 48 gleiche Theile.

Einundfünfzigste Vorlesung.

Abel'sche Gruppen.

§ 507. Durch die allgemeineren Betrachtungen, zu denen wir jetzt übergehen wollen, gewinnen wir einen tieferen Einblick in das Wesen der Abel'schen Gleichungen und in die Methode ihrer Behandlung.

Eine Reihe von unter einander verschiedenen Elementen Θ_1, Θ_2, $\Theta_3, \cdots$ bildet dann eine Gruppe, wenn sie den folgenden Bedingungen genügt:

I) Je zwei Elemente Θ_1 und Θ_2 bestimmen in der angegebenen Reihenfolge eindeutig ein drittes Element der Reihe, welches mit $\Theta_1 \Theta_2$ bezeichnet und durch

$$\Theta_3 = \Theta_1 \Theta_2$$

angedeutet werden möge. Wir sagen Θ_3 sei aus Θ_1 und Θ_2 componirt. Im Allgemeinen ist $\Theta_1 \Theta_2$ von $\Theta_2 \Theta_1$ verschieden. Wir sagen ferner, Θ_3 sei durch linksseitige Composition von Θ_1 an Θ_2 entstanden und durch rechtsseitige Composition von Θ_2 an Θ_1.

II) Für die Operation, durch welche $\Theta_1 \Theta_2$ aus Θ_1 und Θ_2 entspringt, gilt das associative Gesetz (§ 1, Bd. I), d. h. es ist

$$(\Theta_1 \Theta_2)\Theta_4 = \Theta_1(\Theta_2 \Theta_4).$$

III) Aus jeder der beiden Gleichungen

$$\Theta_1 \Theta_4 = \Theta_2 \Theta_4 \quad \text{oder} \quad \Theta_4 \Theta_1 = \Theta_4 \Theta_2$$

folgt $\Theta_1 = \Theta_2$.

Es giebt Gruppen aus unendlich vielen Elementen und solche aus einer endlichen Anzahl. Die ersteren nennen wir unendliche Gruppen; die letzteren nennen wir endliche Gruppen. Da wir uns im Folgenden ausschliesslich mit den letzten beschäftigen, so lassen wir der Einfachheit halber das für uns unnöthige unterscheidende Beiwort weg.

Die Anzahl der Elemente einer Gruppe, d. h. also einer endlichen Gruppe, wollen wir als ihre Ordnung bezeichnen.

Kommen alle Elemente einer Gruppe $\mathfrak{G}_2$ unter den Elementen einer anderen Gruppe $\mathfrak{G}_1$ vor, so heisst $\mathfrak{G}_1$ ein Vielfaches von $\mathfrak{G}_2$, und $\mathfrak{G}_2$ ein Theiler oder Divisor oder eine Untergruppe von $\mathfrak{G}_1$. Der Fall $\mathfrak{G}_1 = \mathfrak{G}_2$ ist in unsere Definition einbegriffen; dabei ist $\mathfrak{G}_2$ ein uneigentlicher Theiler von $\mathfrak{G}_1$.

§ 508. Wir wollen einige elementare Eigenschaften solcher Gruppen herleiten.

A) Lässt man in dem Ausdrucke $\Theta_1 \Theta_x$ oder $\Theta_x \Theta_1$, in welchem Θ_1 ein festes Element von $\mathfrak{G}$ bedeutet, Θ_x alle Elemente der Gruppe durchlaufen, so kommen nach III) wiederum alle Elemente heraus. Folglich giebt es bei jeder Wahl von Θ_1, Θ_2 ein und nur ein Gruppenelement Θ_x und nur ein Θ_y, welche die Gleichungen

$$\Theta_1 \Theta_x = \Theta_2 \quad \text{oder} \quad \Theta_y \Theta_1 = \Theta_2$$

befriedigen.

B) Bilden wir, von einem beliebigen Elemente Θ der Gruppe $\mathfrak{G}$ ausgehend, die Reihe

$$\Theta, \Theta^2, \Theta^3, \Theta^4, \dots \Theta^\varkappa, \dots \Theta^\lambda, \dots,$$

wobei in Folge von II) die einzelnen Potenzen ganz bestimmte Bedeutung haben, so gehören sie wegen I) sämmtlich zu $\mathfrak{G}$. Dann ergiebt sich aus dem Umstande, dass $\mathfrak{G}$ nur eine endliche Anzahl von Elementen besitzt, die Folge, dass Gleichungen von der Form $\Theta^\varkappa = \Theta^\lambda$ bestehen müssen. Ist nun $\lambda = \varkappa + \mu$, dann schliessen wir hieraus

$$\Theta^\varkappa = \Theta^\varkappa \cdot \Theta^\mu \quad \text{und} \quad \Theta^\varkappa = \Theta^\mu \cdot \Theta^\varkappa.$$

Bestimmen wir jetzt Θ_x und Θ_y so, dass für ein beliebiges Θ_0 der Gruppe

$$\Theta_x \Theta^\varkappa = \Theta_0 \quad \text{und} \quad \Theta^\varkappa \Theta_y = \Theta_0$$

wird, dann folgen aus den beiden vorhergehenden Gleichungen, indem man die erste derselben links mit Θ_x und die zweite rechts mit Θ_y componirt, die Relationen

$$\Theta_0 \Theta^\mu = \Theta_0 \quad \text{und} \quad \Theta^\mu \Theta_0 = \Theta_0;$$

d. h. das Element Θ^μ ändert weder durch rechtsseitige noch durch linksseitige Composition ein Element der Gruppe. Wir wollen Θ^μ das **Einheitselement** nennen und mit E bezeichnen. Es giebt nur ein einziges derartiges in einer Gruppe $\mathfrak{G}$; denn wäre H ein anderes von gleicher Eigenschaft, so folgte aus

$$\Theta_0 E = \Theta_0 = \Theta_0 H$$

wegen III) die Identität von E und H.

C) Aus $\Theta^\mu = E$ erkennen wir, dass eine gewisse Potenz jedes Elementes gleich dem Einheitselemente wird. Der niedrigste Exponent, für welchen dies bei Θ eintritt, sei $\varkappa$. Dann zeigt eine schon häufig benutzte Schlussweise, dass alle und nur diejenigen Potenzen von Θ gleich E werden, als deren Exponenten Vielfache von $\varkappa$ auftreten, und dass alle Glieder der Reihe

$$\Theta, \Theta^2, \dots \Theta^{\varkappa-1}, \Theta^\varkappa = E$$

von einander verschieden sind. Wir sagen (vgl. § 295, Bd. I) Θ **gehört zum Exponenten** $\varkappa$ und $\varkappa$ **giebt die Ordnung von** Θ an.

Infolge der Gleichung $\Theta^\varkappa = E$ kann man Potenzen mit negativen Exponenten durch die Definitionsgleichungen

$$\Theta^{-1} = \Theta^{-1} \cdot E = \Theta^{\varkappa-1}, \quad \Theta^{-2} = \Theta^{\varkappa-2}, \dots$$

einführen. Mit Θ gehört auch Θ^{-1} einer Gruppe an, da es gleich einer Potenz von Θ ist.

D) Giebt es in $\mathfrak{G}$ ein Element Θ, welches zu einem bestimmten Exponenten $\varkappa$ gehört, dann giebt es in $\mathfrak{G}$ auch Elemente, die zu einem gegebenen Theiler $\nu = \varkappa : \mu$ von $\varkappa$ gehören. Denn Θ^μ liefert in die ν^{te} Potenz erhoben E; und wenn andrerseits $(\Theta^\mu)^\tau = E$ ist, dann muss $\mu\tau$ ein Vielfaches von $\varkappa$, und also τ ein Vielfaches von ν oder gleich ν sein. Im Allgemeinen ist, wie man an Beispielen sieht, Θ^μ nicht das einzige Element mit dieser Eigenschaft.

E) Es sei $\mathfrak{G}_1$ mit den Elementen $\Theta_1, \Theta_2, \cdots \Theta_m$ ein eigentlicher Theiler einer Gruppe $\mathfrak{G}$ mit den Elementen $\Theta_1, \Theta_2, \cdots \Theta_n$, $(n > m)$, dann lässt sich beweisen, dass m ein Theiler von n ist.

Ist Θ' eins der zu $\mathfrak{G}$ aber nicht zu $\mathfrak{G}_1$ gehörigen Elemente, so bilden wir die Elemente

$$\Theta_1\Theta', \ \Theta_2\Theta', \cdots, \ \Theta_m\Theta'.$$

Diese kommen sämmtlich wegen I) in $\mathfrak{G}$ vor; sie sind ferner von einander verschieden, da aus $\Theta_\alpha\Theta' = \Theta_\beta\Theta'$ nach III) folgen würde $\Theta_\alpha = \Theta_\beta$; sie sind auch von den Elementen der Gruppe $\mathfrak{G}_1$ verschieden, da aus $\Theta_\alpha\Theta' = \Theta_\beta$ nach C) und III) $\Theta' = \Theta_\alpha^{-1}\Theta_\beta$ folgen würde, so dass Θ' selbst schon gegen die Annahme der Gruppe $\mathfrak{G}_1$ angehörte.

$\mathfrak{G}$ umfasst also mindestens $2m$ Elemente. Besitzt $\mathfrak{G}$ ausser diesen Elementen Θ_α und $\Theta_\alpha\Theta'$ noch ein weiteres Element Θ'', dann bilden wir mit seiner Hülfe ebenso

$$\Theta_1\Theta'', \ \Theta_2\Theta'', \cdots, \ \Theta_m\Theta''$$

und führen dieselben Schlüsse durch wie oben, aus denen sich ergiebt, dass $\mathfrak{G}$ auch alle diese neuen m Elemente enthält; dass diese untereinander und dass sie von den früheren $2m$ Elementen verschieden sind. $\mathfrak{G}$ umfasst also mindestens $3m$ Elemente. — So fahren wir fort und erkennen: Die Ordnung des Theilers einer Gruppe ist ein Theiler der Ordnung der Gruppe.

Die von einander verschiedenen Potenzen eines beliebigen Elementes Θ von $\mathfrak{G}$ bilden für sich einen eigentlichen Theiler von $\mathfrak{G}$, wenn sie nicht $\mathfrak{G}$ selbst erschöpfen. Die Ordnung dieses Theilers ist mit der Ordnung des Elementes identisch (vgl. C). Daher ist die Ordnung jedes Elementes ein Theiler der Ordnung der Gruppe. —

Es liegt nicht in dem Plane dieser Vorlesungen, die Theorie der oben definirten, allgemeinen (endlichen) Gruppen eingehend zu behandeln. Nachdem wir in diesem Paragraphen die elementarsten Gruppeneigenschaften hergeleitet haben, wenden wir uns zu einer ganz besonders einfachen Art von Gruppen.

§ 509. In II) haben wir erwähnt, dass $\Theta_1\Theta_2$ im Allgemeinen von $\Theta_2\Theta_1$ verschieden sei. Wir wollen nun die Vertauschbarkeit der Elemente in einer Composition zu den Voraussetzungen hinzunehmen.

IV) Eine Gruppe heisst eine Abel'sche Gruppe, wenn für alle ihre Operationen das commutative Gesetz (§ 1, Bd. I) gilt, d. h. wenn $\Theta_1\Theta_2 = \Theta_2\Theta_1$ ist. Aus diesem Grunde heisst eine Abel'sche Gruppe auch eine Gruppe vertauschbarer Elemente. — Die Regeln der Composition entsprechen in diesem Falle denen der gewöhnlichen Multiplication; wir werden deshalb auch hier von Product und von Potenz sprechen dürfen.

Die besonderen Gesetze, denen die Abel'schen Gruppen unterworfen sind, wurden von E. Schering*), von L. Kronecker**) und besonders eingehend von G. Frobenius und L. Stickelberger***) untersucht. Wir leiten die für unsere Zwecke wichtigsten Resultate hier ab und schliessen uns dabei im Allgemeinen an die letztgenannten Untersuchungen an†).

F) Da für zwei beliebige Elemente der Abel'schen Gruppe $\mathfrak{A}$ das commutative Gesetz gilt, so gilt es auch (§ 1, Bd. I) für das Resultat der Composition beliebig vieler Elemente. Für die Potenzerhebung eines Productes hat man also im Besonderen

$$(\Theta_1\Theta_2\Theta_3\cdots)^\alpha = \Theta_1^\alpha\Theta_2^\alpha\Theta_3^\alpha\cdots.$$

G) Wenn die beiden Exponenten ϱ und σ, zu denen bez. die Elemente Θ_1 und Θ_2 gehören sollen, theilerfremde Zahlen sind, dann gehört das Product $\Theta_1\Theta_2$ zu dem Exponenten $\varrho\sigma$. Denn bezeichnen wir mit τ den Exponenten, zu welchem $\Theta_1\Theta_2$ gehört, so ist $(\Theta_1\Theta_2)^\tau = E$, und also um so mehr auch

$$(\Theta_1\Theta_2)^{\varrho\tau} = \Theta_1^{\varrho\tau}\Theta_2^{\varrho\tau} = \Theta_2^{\varrho\tau} = E, \qquad \text{da} \quad \Theta_1^\varrho = E \quad \text{ist},$$
$$(\Theta_1\Theta_2)^{\sigma\tau} = \Theta_1^{\sigma\tau}\Theta_2^{\sigma\tau} = \Theta_1^{\sigma\tau} = E, \qquad \text{da} \quad \Theta_2^\sigma = E \quad \text{ist};$$

demnach ist $\varrho\tau$ ein Vielfaches von σ, und also, weil ϱ und σ theilerfremd sind, τ selbst ein Vielfaches von σ. Aus der zweiten Gleichungsreihe folgt ebenso, dass τ ein Vielfaches von ϱ sei. Folglich ist τ ein Vielfaches von $\varrho\sigma$. Da weiter aber $(\Theta_1\Theta_2)^{\varrho\sigma} = E$ ist, so gehört $\Theta_1\Theta_2$ schon zum Exponenten $\varrho\sigma$ selbst.

H) Ist n_1 die kleinste Zahl, welche die sämmtlichen zu den Elementen von $\mathfrak{A}$ gehörigen Exponenten zu Theilern hat, dann giebt es

*) Gött. Abhandl. 14 (1869). Math. Cl. p. 3.

**) Berl. Ber. (1870), 1. Dec., p. 881.

***) J. f. M. 86 (1879), p. 217.

†) Es sei auch auf die inhaltreiche Abhandlung von K. Zsigmondy, Monatshefte f. Math. 7 (1896), p. 185, hingewiesen.

in $\mathfrak{A}$ auch Elemente, welche zu n_1 selbst gehören. Denn wenn n_1 in seine Primfactoren aufgelöst $= p^\alpha q^\beta \cdots$ ist, so giebt es nach der Annahme über n_1 sicher ein Θ, welches zu einem durch p^α theilbaren Exponenten gehört, also nach D) auch ein Element Θ_a, welches zu p^α selbst gehört; ebenso findet man ein zu q^β gehöriges Θ_b, u. s. f. Also gehört nach G) das Element $\Theta_a \Theta_b \cdots$ zu n_1 selbst. Die Zahl n_1 nennen wir die erste Invariante der Abel'schen Gruppe $\mathfrak{A}$.

Da n_1 ein ganzes Vielfaches jedes in $\mathfrak{A}$ vorkommenden Exponenten ist, so wird für jedes Element Θ von $\mathfrak{A}$ die Gleichung $\Theta^{n_1} = E$ gelten.

J) Ist Θ_1 eins der zu n_1 gehörigen Elemente von $\mathfrak{A}$, und erschöpfen die untereinander verschiedenen Potenzen von Θ, nämlich

$$(1) \qquad \Theta_1, \; \Theta_1^2, \; \Theta_1^3, \; \cdots \; \Theta_1^{n_1 - 1}, \; \Theta_1^{n_1} = E$$

noch nicht alle n Elemente der Gruppe $\mathfrak{A}$, dann sei Θ_α eins der übrigen Elemente; wir bilden die Reihe der Producte

$$(2) \qquad \Theta_\alpha, \; \Theta_\alpha \Theta_1, \; \Theta_\alpha \Theta_1^2, \; \cdots \; \Theta_\alpha \Theta_1^{n_1 - 1}$$

und benutzen die in E) abgeleiteten Resultate; ebenso gehen wir, wenn es nöthig ist, weiter zu

$$(3) \qquad \Theta_\beta, \; \Theta_\beta \Theta_1, \; \Theta_\beta \Theta_1^2, \; \cdots \; \Theta_\beta \Theta_1^{n_1 - 1}$$

u. s. f.

Jede der Zeilen (1), (2), (3), $\cdots$ fassen wir nun als ein Element auf; wir setzen (1) gleich H_1, (2) gleich H_α, (3) gleich H_β, u. s. f. und definiren die Composition der H derart, dass wir setzen

$$H_\alpha H_\beta = H_\gamma, \quad \text{wenn} \quad (\Theta_\alpha \Theta_1^\varkappa)(\Theta_\beta \Theta_1^\lambda) = \Theta_\alpha \Theta_\beta \cdot \Theta_1^\mu = \Theta_\gamma \Theta_1^\nu$$

ist. Dies ist eine erlaubte Definition, da ja in der letzten Gleichung der Index γ von α und β allein, aber nicht von $\varkappa$ und λ abhängig ist. Es wird also H_γ eindeutig durch H_α und H_β bestimmt (§ 507, I). — Aus $(\Theta_\alpha \Theta_\beta)\Theta_\delta = \Theta_\alpha(\Theta_\beta \Theta_\delta)$ folgt ferner $(H_\alpha H_\beta) H_\delta = H_\alpha (H_\beta H_\delta)$, d. h. es gilt das commutative Gesetz (II, § 507). — Ist weiter

$$H_\alpha H_\beta = H_\alpha H_\delta, \quad \text{so ist} \quad (\Theta_\alpha \Theta_1^\varkappa)(\Theta_\beta \Theta_1^\lambda) = (\Theta_\alpha \Theta_1^\mu)(\Theta_\delta \Theta_1^\nu);$$

weil sich nun aus der letzten Gleichung $\Theta_\delta = \Theta_\beta \Theta_1^\sigma$ ergiebt, so ist $H_\beta = H_\delta$, wie III, § 507 es fordert. — Endlich besteht wegen der Vertauschbarkeit der Θ auch diejenige der H, d. h. die H bilden eine Abel'sche Gruppe (IV, § 506). Wir wollen sie $\mathfrak{A}_1$ nennen.

In $\mathfrak{A}_1$ repräsentirt H_1 das Einheitselement, welches wir mit E_1 bezeichnen; denn aus

$$\Theta_\alpha E = \Theta_\alpha \quad \text{folgt} \quad H_\alpha E_1 = E_1 H_\alpha = H_\alpha .$$

Es gelten in der Gruppe $\mathfrak{A}_1$ der H alle in H) abgeleiteten Eigenschaften, und demnach existirt eine kleinste Zahl n_2, für welche jedes Element H von $\mathfrak{A}_1$ die Gleichung $H^{n_2} = E_1$ befriedigt. Geht man zu den Θ zurück, so kommt man auf das Bestehen der Gleichungen

$$(\Theta_\alpha \Theta_1^x)^{n_2} = \Theta_1^\lambda \quad \text{oder} \quad \Theta_\alpha^{n_2} = \Theta_1^\mu$$

für jedes Θ_α von $\mathfrak{A}$ und passendes μ; d. h. jedes Element Θ_α von $\mathfrak{A}$ giebt in die n_2^{te} Potenz erhoben eine Potenz von Θ_1..

Da n_2 die erste Invariante von $\mathfrak{A}_1$ ist, so giebt es ein zu n_2 gehöriges Element H'; und wenn daher Θ' zu der Reihe gehört, welche von H' repräsentirt wird, so ist Θ'^{n_2} auch die niedrigste Potenz von Θ', welche zu einer Potenz von Θ_1 wird. Dann folgt nach bekannten Schlüssen, dass

$$\Theta'^{n_2}, \; \Theta'^{2n_2}, \; \Theta'^{3n_2}, \; \ldots$$

seine einzigen Potenzen dieser Eigenschaft sind; und weil $\Theta'^{n_1} = E$ ist, so muss n_2 ein Theiler von n_1 sein, der freilich auch n_1 selbst werden kann. Erheben wir

$$\Theta'^{n_2} = \Theta_1^\mu$$

in die $(n_1 : n_2)^{\text{te}}$ Potenz, so folgt

$$\Theta'^{n_1} = E = \Theta_1^{\frac{\mu n_1}{n_2}};$$

aus dieser Relation geht hervor, dass $(\mu : n_2)$ eine ganze Zahl ist,

$$\mu = n_2 m.$$

Dann ergiebt sich für das Element

$$\Theta_2 = \Theta' \Theta_1^{n_1 - m},$$

welches natürlich auch zu H' gehört, dass erst seine n_2^{te} Potenz eine Potenz von Θ_1 wird; es gilt daher die Gleichung

$$\Theta_2^{n_2} = \Theta'^{n_2} \Theta_1^{n_1 n_2 - n_2 m} = \Theta'^{n_2} \Theta_1^{n_1 n_2 - \mu} = \Theta_1^{n_1 n_2} = E.$$

Es giebt also ein kleinstes n_2 so, dass n_2 ein eigentlicher oder uneigentlicher Theiler von n_1 ist; dass jedes Θ in die n_2^{te} Potenz erhoben eine Potenz von Θ_1 wird; und dass ein Θ_2 zu n_2 gehört, für welches die n_2^{te} Potenz direct gleich E ist. Alle $n_1 n_2$ Potenzproducte, welche mit Hülfe von Θ_1 und Θ_2 gebildet werden können, nämlich

$$(4) \qquad \Theta_1^\alpha \Theta_2^\beta \qquad (\alpha = 1, 2, \cdots n_1; \; \beta = 1, 2, \cdots n_2),$$

sind von einander verschieden. Denn aus der Annahme

$$\Theta_1^\alpha \Theta_2^\beta = \Theta_1^\gamma \Theta_2^\delta \qquad (\alpha, \gamma \leqq n_1; \; \beta, \delta \leqq n_2; \; \beta \geqq \delta)$$

folgt ja sofort

$$\Theta_2^{\beta - \delta} = \Theta_1^{\gamma - \alpha},$$

und also, da $(\beta - \delta)$ nicht grösser als $(n_1 - 1)$ sein kann, $\beta = \delta$; $\gamma = \alpha$.

Erschöpfen die $n_1 n_2$ Elemente (4) noch nicht alle Elemente von $\mathfrak{A}$, dann können wir eine neue Abel'sche Gruppe $\mathfrak{A}_2$ herstellen, deren Einheitselement der Inbegriff der Elemente (4) ist, und deren andere Elemente je durch den Inbegriff von $n_1 \cdot n_2$ Elementen, die mit Hülfe eines neuen Θ_x von $\mathfrak{A}$ gebildet sind

(5) $$\Theta_x \Theta_1^\alpha \Theta_2^\beta \qquad (\alpha = 1, 2, \cdots n_1;\ \beta = 1, 2, \cdots n_2),$$

dargestellt werden. Die Composition für $\mathfrak{A}_2$ wird dabei wie oben bei $\mathfrak{A}_1$ definirt. Für $\mathfrak{A}_2$ giebt es eine Zahl n_3 derart, dass jedes Element in die n_3^{te} Potenz erhoben das Einheitselement von $\mathfrak{A}_2$ giebt; n_3 ist ein Theiler von n_2; es giebt in $\mathfrak{A}_2$ ein zu n_3 gehöriges Element. Folglich giebt es in $\mathfrak{A}_1$ ein Θ'', dessen n_3^{te} Potenz zu (4) gehört; daraus lässt sich ein Θ_3 in $\mathfrak{A}$ herleiten, dessen n_3^{te} Potenz $= E$ ist. Alle $n_1 n_2 n_3$ Elemente

(6) $$\Theta_1^\alpha \Theta_2^\beta \Theta_3^\gamma \qquad (\alpha = 1, \cdots n_1;\ \beta = 1, \cdots n_2;\ \gamma = 1, \cdots n_3)$$

sind von einander verschieden.

Durch Fortsetzung dieses Verfahrens kommt man zu dem Hauptresultate: I n j e d e r A b e l ' s c h e n G r u p p e $\mathfrak{A}$ v o n n E l e m e n t e n k a n n m a n e i n S y s t e m v o n r E l e m e n t e n

(6ᵃ) $$\Theta_1,\ \Theta_2,\ \cdots\ \Theta_{r-1},\ \Theta_r$$

m i t d e n z u g e h ö r i g e n E x p o n e n t e n

(6ᵇ) $$n_1,\ n_2,\ \cdots\ n_{r-1},\ n_r \qquad (n_{\alpha+1} \text{ theilt } n_\alpha;\ n_r > 1)$$

m i t f o l g e n d e n E i g e n s c h a f t e n b e s t i m m e n: J e d e d e r P o t e n z e n $\Theta_\alpha^{n_\alpha}$ w i r d d e m E i n h e i t s e l e m e n t e g l e i c h, a b e r k e i n e n i e d e r e P o t e n z v o n Θ_α; g l e i c h z e i t i g i s t $\Theta_\alpha^{n_\alpha}$ d i e n i e d r i g s t e P o t e n z, w e l c h e a l s P o t e n z p r o d u c t d e r v o r h e r g e h e n d e n E l e m e n t e

(7) $$\Theta_1^{x_1} \Theta_2^{x_2} \cdots \Theta_{\alpha-1}^{x_{\alpha-1}}$$

d a r s t e l l b a r i s t; j e d e s E l e m e n t Θ d e r A b e l ' s c h e n G r u p p e i s t e i n d e u t i g i n d e r F o r m

(8) $$\Theta = \Theta_1^{\lambda_1} \Theta_2^{\lambda_2} \cdots \Theta_r^{\lambda_r} \qquad (\lambda_\alpha < n_\alpha)$$

a u s d r ü c k b a r; e i n e G l e i c h u n g v o n d e r F o r m

(9) $$\Theta_1^{\mu_1} \Theta_2^{\mu_2} \cdots \Theta_r^{\mu_r} = \Theta_1^{\nu_1} \Theta_2^{\nu_2} \cdots \Theta_r^{\nu_r}$$

k a n n n u r d a n n b e s t e h e n, w e n n j e d e s $(\mu_\alpha - \nu_\alpha)$ e i n V i e l f a c h e s v o n n_α i s t. M a n h a t

(10) $$n = n_1 n_2 \cdots n_r.$$

Wir nennen ein jedes solche System $\Theta_1, \Theta_2, \cdots \Theta_r$ eine **Basis der Abel'schen Gruppe.** $\Theta_1, \Theta_2, \cdots \Theta_r$ bilden eine Basis, wenn sie folgende Eigenschaften haben:

1) Jedes Element von $\mathfrak{A}$ kann auf die Form $\Theta_1^{\lambda_1}\Theta_2^{\lambda_2}\cdots\Theta_r^{\lambda_r}$ gebracht werden.
2) Die Gleichung $\Theta_1^{\mu_1}\Theta_2^{\mu_2}\cdots\Theta_r^{\mu_r} = E$ fordert, dass jedes $\Theta_\alpha^{\mu_\alpha} = E$ ist.
3) Gehört Θ_α zum Exponenten n_α, so ist n_α durch $n_{\alpha+1}$ theilbar, und $n_r > 1$.

Die Zahlen $n_1, n_2, \cdots n_r$ heissen die erste, zweite, $\cdots$ r^{te} Invariante von $\mathfrak{A}$. Diese Bezeichnung wird noch gerechtfertigt werden müssen (§ 513).

§ 510. Zunächst benutzen wir den abgeleiteten Hauptsatz zur Berechnung der Anzahl derjenigen Elemente von $\mathfrak{A}$, welche zu einem vorgegebenen Theiler m von n als Exponenten gehören. Wir bezeichnen diese Zahl durch $\psi(m)$.

Bedeuten a und b theilerfremde Zahlen, so ist

$$\psi(ab) = \psi(a)\psi(b).$$

Dies beweisen wir folgendermassen: Damit das Element

$$\Theta_1^{a_1}\Theta_2^{a_2}\cdots\Theta_r^{a_r} \tag{11}$$

zum Exponenten a gehöre, muss zunächst

$$\left(\Theta_1^{a_1}\Theta_2^{a_2}\cdots\Theta_r^{a_r}\right)^a = E$$

sein, d. h. wir können setzen

$$aa_1 = n_1\alpha_1,\quad aa_2 = n_2\alpha_2,\quad \cdots,\quad aa_r = n_r\alpha_r, \tag{12}$$

wobei $\alpha_1, \alpha_2, \cdots \alpha_r$ ganze, positive Zahlen bedeuten. Damit ferner keine niedere Potenz als die a^{te} dem Einheitselemente gleich wird, muss der grösste gemeinsame Theiler von $\alpha_1, \alpha_2, \cdots \alpha_r$ zu a theilerfremd sein; denn wäre das nicht der Fall, sondern wäre dieser gemeinsame Theiler δ von $\alpha_1, \alpha_2, \cdots \alpha_r, a$ grösser als 1, dann wären schon die Producte

$$a_1\frac{a}{\delta} = n_1\frac{\alpha_1}{\delta},\quad a_2\frac{a}{\delta} = n_2\frac{\alpha_2}{\delta},\quad \cdots\quad a_r\frac{a}{\delta} = n_r\frac{\alpha_r}{\delta}$$

ganze Vielfache von $n_1, n_2, \cdots n_r$, und es würde demnach bereits die $\left(\frac{a}{\delta}\right)^{\text{te}}$ Potenz von (11) gleich E werden.

Ebenso können wir, wenn das Potenzproduct

$$\Theta_1^{b_1}\Theta_2^{b_2}\cdots\Theta_r^{b_r} \tag{11a}$$

zum Exponenten b gehört, die Gleichungen

$$(12^a) \qquad bb_1 = n_1\beta_1, \quad bb_2 = n_2\beta_2, \quad \cdots \quad bb_r = n_r\beta_r$$

ansetzen, wobei $\beta_1, \beta_2, \cdots \beta_r; b$ den gemeinsamen Theiler 1 haben.

Nun betrachten wir das aus (11) und (11ᵃ) componirte Element

$$(13) \quad \Theta_1^{a_1+b_1}\Theta_2^{a_2+b_2}\cdots\Theta_r^{a_r+b_r} = \left(\Theta_1^{a_1}\Theta_2^{a_2}\cdots\Theta_r^{a_r}\right)\left(\Theta_1^{b_1}\Theta_2^{b_2}\cdots\Theta_r^{b_r}\right)$$

und erkennen aus der zweiten Form, dass die $(ab)^{\text{te}}$ Potenz von (13) gleich E wird. Heisst jetzt $\varkappa$ der Exponent, zu dem (13) gehört, so wird

$(a_1 + b_1)\varkappa$ durch n_1; $(a_2 + b_2)\varkappa$ durch n_2; $\cdots$; $(a_r + b_r)\varkappa$ durch n_r, also

$a\beta_1(a_1 + b_1)\varkappa$ durch $\beta_1 n_1 = bb_1$; $a\beta_2(a_2 + b_2)\varkappa$ durch $\beta_2 n_2 = bb_2$; $\cdots$

theilbar; und da $aa_1 = n_1\alpha_1, \cdots$ ist, so müsste

$$a\beta_1 b_1\varkappa \text{ durch } bb_1; \quad a\beta_2 b_2\varkappa \text{ durch } bb_2; \;\cdots,$$

d. h.

$$a\beta_1\varkappa \quad \text{„} \quad b; \quad a\beta_2\varkappa \quad \text{„} \quad b; \;\cdots,$$

und weil a zu b theilerfremd ist, endlich auch jede der Grössen

$$\beta_1\varkappa; \; \beta_2\varkappa; \;\cdots\; \beta_r\varkappa \text{ durch } b$$

theilbar sein. Der grösste gemeinsame Theiler von $\beta_1, \beta_2, \cdots \beta_r$ war zu b theilerfremd; daher ist $\varkappa$ durch b theilbar. Ebenso folgt, dass $\varkappa$ durch a theilbar ist; der Voraussetzung nach sind a und b theilerfremd; demnach ist $\varkappa$ durch ab theilbar, und das componirte Element (13) gehört zu ab. Hiermit ist als erstes Zwischenresultat bewiesen, dass das Product zweier zu a bez. zu b gehöriger Elemente Θ selbst zu dem Exponenten ab gehört, wenn a und b theilerfremd sind.

Umgekehrt wollen wir nachweisen: Wenn ein Element

$$(13^a) \qquad \Theta_1^{t_1}\Theta_2^{t_2}\cdots\Theta_r^{t_r}$$

zu ab gehört, wobei a und b theilerfremd zu einander sein sollen, dann kann man die positiven Zahlen $a_1, a_2, \cdots a_r$ und $b_1, b_2, \cdots b_r$ so bestimmen, dass

$$(14) \qquad t_1 = a_1 + b_1; \quad t_2 = a_2 + b_2; \quad \cdots \quad t_r = a_r + b_r$$

wird, und dass die dadurch festgelegten Ausdrücke (11) und (11ᵃ) zu a und bezw. zu b gehören. $t_1, t_2, \cdots t_r$ müssen, wie in der Voraussetzung eingeschlossen liegt, so beschaffen sein, dass

$$t_1 ab = n_1\tau_1; \quad t_2 ab = n_2\tau_2; \quad \cdots \quad t_r ab = n_r\tau_r$$

wird, und dass die $r + 1$ Zahlen $\tau_1, \tau_2, \cdots \tau_r; ab$ theilerfremd sind.

Wir können stets nach einer elementaren Methode der Zahlentheorie die Zerfällungen der τ in die Formen

(15) $\tau_1 = \alpha_1 b + \beta_1 a; \quad \tau_2 = \alpha_2 b + \beta_2 a; \quad \cdots \quad \tau_r = \alpha_r b + \beta_r a$

durchführen. Es ist ersichtlich, dass weder $\beta_1, \beta_2, \cdots \beta_r, b$ noch $\alpha_1, \alpha_2, \cdots \alpha_r, a$ einen gemeinsamen Theiler haben; denn die $\tau_1, \tau_2, \cdots \tau_r$ würden denselben besitzen. Nun ist für jedes $\lambda = 1, 2, \cdots r$ die Gleichung befriedigt

$$\tau_\lambda n_\lambda = t_\lambda ab = \alpha_\lambda b n_\lambda + \beta_\lambda a n_\lambda,$$

und da $t_\lambda ab$ und $\alpha_\lambda b n_\lambda$ durch b theilbar sind, so muss auch $\beta_\lambda a n_\lambda$ durch b theilbar sein; deshalb ist auch $\beta_\lambda n_\lambda$ durch b theilbar, weil a und b theilerfremd sind. Wir können demnach setzen

$$\beta_1 n_1 = b b_1, \quad \beta_2 n_2 = b b_2, \quad \cdots \quad \beta_r n_r = b b_r.$$

Aus ähnlichen Gründen ergiebt sich das entsprechende Resultat

$$\alpha_1 n_1 = a a_1, \quad \alpha_2 n_2 = a a_2, \quad \cdots \quad \alpha_r n_r = a a_r$$

mit ganzzahligen $a_1, a_2, \cdots a_r; b_1, b_2, \cdots b_r$. Für die so gefundenen Zahlen a_λ und b_λ ist wegen (12) und (12ᵃ)

$$ab(a_\lambda + b_\lambda) = n_\lambda(\alpha_\lambda b + \beta_\lambda a) = n_\lambda \tau_\lambda = ab t_\lambda.$$

Daher ist die Forderungsreihe (14) befriedigt. Hiermit ist als zweites Zwischenresultat bewiesen, dass jedes zu ab gehörige Element Θ' aus zwei anderen componirt werden kann, die zu a und bez. zu b gehören.

Es fragt sich nun endlich, auf wie viele verschiedene Arten eine solche Zerlegung (14) bei (13ᵃ) möglich sei. Befriedigen auch $\alpha'_\lambda, \beta'_\lambda$ $(\lambda = 1, 2, \cdots r)$ die Forderungen (15), so wird, wie aus den Elementen der Zahlentheorie bekannt ist, bei beliebigen ganzzahligen m_λ

$$\begin{aligned}
\alpha'_\lambda &= \alpha_\lambda + a m_\lambda, & \beta'_\lambda &= \beta_\lambda - b m_\lambda;\\
\alpha'_\lambda n_\lambda &= \alpha_\lambda n_\lambda + a n_\lambda m_\lambda, & \beta'_\lambda n_\lambda &= \beta_\lambda n_\lambda - b n_\lambda m_\lambda;\\
a'_\lambda a &= a_\lambda a + a n_\lambda m_\lambda, & b'_\lambda b &= b_\lambda b - b n_\lambda m_\lambda;\\
a'_\lambda &= a_\lambda + n_\lambda m_\lambda, & b'_\lambda &= b_\lambda - n_\lambda m_\lambda.
\end{aligned}$$

Hiernach kann man auf eine und nur auf eine Art a'_λ so bestimmen, dass a'_λ kleiner als n_λ wird; dadurch ergiebt sich dann sofort wegen der Gleichungen, die dem Systeme (14) entsprechen, dass

$$b'_\lambda \text{ entweder } = (t_\lambda - a'_\lambda) \text{ oder } = n_\lambda - (a'_\lambda - t_\lambda)$$

auch eindeutig bestimmt, kleiner als n_λ und positiv wird. Die durchgeführte Zerlegung ist also nur auf eine Art möglich.

Damit ist das zu Beginn des Paragraphen ausgesprochene Theorem bewiesen.

§ 511. Die Untersuchung von $\psi(m)$ ist jetzt also auf diejenige einfachere von $\psi(p^\alpha)$ zurückgeführt, wobei p^α eine in n_1 vorkommende Primzahlpotenz bedeutet. Um diese Frage zu erledigen, setzen wir die r Invarianten $n_1, n_2, \cdots n_r$ der Gruppe $\mathfrak{A}$ in die Form

$$(16) \qquad n_1 = \nu_1 p^{\alpha_1}; \quad n_2 = \nu_2 p^{\alpha_2}; \quad \cdots \quad n_r = \nu_r p^{\alpha_r},$$

so dass die ν_λ zu p theilerfremd geworden sind. Es sei dabei das Grössenverhältniss von α zu den Exponenten $\alpha_1, \alpha_2, \cdots \alpha_r$ bestimmt durch

$$(16^a) \qquad \alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_\varkappa \geqq \alpha > \alpha_{\varkappa+1} \geqq \alpha_{\varkappa+2} \geqq \cdots \geqq \alpha_r.$$

Diese Folge ist aus dem Grunde möglich, weil n_ϱ durch $n_{\varrho+1}$ theilbar, und also jedes folgende α_λ höchstens so gross ist, wie das vorhergehende.

Soll nun ein $\Theta_1^{\mu_1}\Theta_2^{\mu_2}\cdots\Theta_r^{\mu_r}$ so beschaffen sein, dass die Potenz

$$\left(\Theta_1^{\mu_1}\Theta_2^{\mu_2}\cdots\Theta_r^{\mu_r}\right)^{p^\alpha} = \Theta_1^{\mu_1 p^\alpha}\Theta_2^{\mu_2 p^\alpha}\cdots\Theta_r^{\mu_r p^\alpha} = E$$

wird, dann müssen $\mu_1 p^\alpha, \mu_2 p^\alpha, \cdots$ bezw. durch $\nu_1 p^{\alpha_1}, \nu_2 p^{\alpha_2}, \cdots$ und also $\mu_1, \mu_2, \cdots$ bezw. durch $\nu_1, \nu_2, \cdots$ theilbar sein. Setzen wir deshalb zu Abkürzung

$$\Theta_1^{\nu_1} = \tau_1, \quad \Theta_2^{\nu_2} = \tau_2, \quad \cdots \quad \Theta_r^{\nu_r} = \tau_r \qquad \left(\tau_\lambda \text{ gehört zu } p^{\alpha_\lambda}\right),$$

dann muss jedes zu p^α gehörige Element in die Form gebracht werden können

$$\tau_1^{\sigma_1}\tau_2^{\sigma_2}\cdots\tau_r^{\sigma_r},$$

und wir brauchen nur zu fragen, welchen Bedingungen die $\sigma_1, \sigma_2, \cdots \sigma_r$ zu unterwerfen sind, damit die Potenz

$$\left(\tau_1^{\sigma_1}\tau_2^{\sigma_2}\cdots\tau_r^{\sigma_r}\right)^{p^\alpha} = \tau_1^{\sigma_1 p^\alpha}\tau_2^{\sigma_2 p^\alpha}\cdots\tau_r^{\sigma_r p^\alpha} = E$$

wird. Da $\tau_{\varkappa+1}$ zu $p^{\alpha_{\varkappa+1}}$ gehört, und da $\alpha > \alpha_{\varkappa+1} \geqq \alpha_{\varkappa+2} \geqq \cdots$ ist, so kann man $\sigma_{\varkappa+1}$ gleich einer beliebigen unter den Zahlen $0, 1, \cdots p^{\alpha_{\varkappa+1}-1}$ wählen und ähnlich $\sigma_{\varkappa+2}, \cdots$. Die Anzahl der Möglichkeiten für $\sigma_{\varkappa+1}, \cdots \sigma_r$ beträgt also insgesammt

$$p^{\alpha_{\varkappa+1}+\alpha_{\varkappa+2}+\cdots+\alpha_r}.$$

Für σ_1 muss ein Vielfaches von $p^{\alpha_1-\alpha}$ eintreten, d. h. man darf für σ nur ein $p^{\alpha_1-\alpha}, 2p^{\alpha_1-\alpha}, \cdots p^\alpha \cdot p^{\alpha_1-\alpha}$ als Werth annehmen, und Aehnliches gilt für $\sigma_2, \cdots \sigma_\varkappa$. Die Anzahl der Möglichkeiten hierfür beträgt also $p^{\alpha\varkappa}$. Bei dieser letzten Sorte ist aber zu bedenken, dass auch erst die $p^{\alpha\text{te}}$ Potenz gleich E werden darf; es ist also auszuschliessen, dass alle $\varkappa$ Werthe von $\sigma_1, \sigma_2, \cdots \sigma_\varkappa$ gleichzeitig durch

$p^{\alpha_1-\alpha+1}, p^{\alpha_2-\alpha+1}, \cdots$ theilbar sind; denn in diesem Falle wäre schon die $p^{\alpha-1\text{te}}$ Potenz gleich E. Es bleiben also für $\sigma_1, \sigma_2, \cdots \sigma_\varkappa$ nur

$$p^{\alpha\varkappa} - p^{(\alpha-1)\varkappa}$$

Werthsysteme zurück. Es sind demnach im Ganzen

$$(17) \qquad p^{\alpha\varkappa}\left(1-\frac{1}{p^\varkappa}\right)p^{\alpha_{\varkappa+1}+\alpha_{\varkappa+2}+\cdots+\alpha_r}$$

Elemente in $\mathfrak{A}$ vorhanden, die zum Exponenten p^α gehören. Die Anzahl aller Elemente, welche zu p^{α_r} gehören, beträgt daher insbesondere

$$p^{r\alpha_r}\left(1-\frac{1}{p^r}\right).$$

§ 512. Im Anschlusse an dieses Resultat suchen wir die Anzahl der Elemente von $\mathfrak{A}$, die zu einer der Zahlen $p^\alpha, p^{\alpha-1}, \cdots p^2, p^1, 1$ als Exponenten gehören. Diese Anzahl wollen wir mit $\chi(p^\alpha)$ bezeichnen. Hierbei bleibt die obige Bestimmung von $\sigma_{\varkappa+1}, \sigma_{\varkappa+2}, \cdots$ ungeändert, während bei der Bestimmung von $\sigma_1, \sigma_2, \cdots \sigma_\varkappa$ zu beachten ist, dass jetzt keine Exponentensysteme ausgeschlossen zu werden brauchen. In (17) ist also einfach das negative Glied der Klammergrösse zu unterdrücken. Es ist

$$(17^a) \qquad \chi(p^\alpha) = p^{\alpha\varkappa+\alpha_{\varkappa+1}+\cdots+\alpha_r},$$

d. h. dies ist die Anzahl der Elemente in $\mathfrak{A}$, welche zu einer der Potenzen $1, p, \cdots p^\alpha$ als Exponenten gehören. Es ist also insbesondere

$$(17^b) \qquad \chi(p^{\alpha_1}) = p^{\alpha_1+\alpha_2+\cdots+\alpha_r}; \quad \chi(p^{\alpha_r}) = p^{r\alpha_r}.$$

Wir brauchen noch eine Umformung unserer Resultate und führen dazu gewisse Grössen $q_0, q_1, q_2, \cdots$ ein. Es sei q_0 die Anzahl derjenigen Glieder der Reihe

$$n_1, n_2, n_3, \cdots n_r,$$

welche durch p gar nicht, q_α die Anzahl derjenigen Glieder ($\alpha = 1, 2, \cdots$), welche durch p^α, aber nicht durch eine höhere Potenz von p theilbar sind.

Dann giebt $\varkappa$ in (16^a) an, wie viele der $\alpha_1, \alpha_2, \cdots$ grösser oder gleich α sind, d. h. es ist

$$\varkappa = q_\alpha + q_{\alpha+1} + \cdots + q_{\alpha_1}.$$

Setzen wir ferner

$$\chi(p^{\alpha-1}) = p^{(\alpha-1)\lambda+\alpha_{\lambda+1}+\cdots+\alpha_r},$$

so ist ebenso

$$\lambda = q_{\alpha-1} + q_\alpha + \cdots + q_{\alpha_1}.$$

Nun ist aber nur dann $\lambda > \varkappa$, wenn

$$\alpha - 1 = \alpha_{\varkappa+1} = \alpha_{\varkappa+2} = \cdots = \alpha_{\varkappa+\varrho}$$

ist, und zwar wird dabei

$$\lambda - \varkappa = q_{\alpha-1} = \varrho.$$

Dies ergiebt dann

$$\frac{\chi(p^\alpha)}{\chi(p^{\alpha-1})} = p^{\alpha\varkappa - (\alpha-1)\lambda + \alpha_{\varkappa+1} + \cdots + \alpha_\lambda} = p^{\alpha\varkappa - (\alpha-1)(\varkappa+\varrho) + (\alpha-1)\varrho} = p^\varkappa$$
$$= p^{q_\alpha + q_{\alpha+1} + \cdots + q_{\alpha_1}}.$$

Wir bemerken ferner noch, dass

$$q_0 + q_1 + q_2 + \cdots + q_{\alpha_1} = r$$

ist, wie man aus dem Umstande erkennt, dass beide Seiten die Anzahl sämmtlicher n_α geben; und weiter, wenn man die einander gleichen Zahlen in der Reihe $\alpha_1, \alpha_2, \cdots \alpha_r$ zusammenfasst, dass

$$q_1 + 2q_2 + 3q_3 + \cdots + \alpha_1 q_{\alpha_1} = \alpha_1 + \alpha_2 + \cdots + \alpha_r$$

wird. Diese letztere Anzahl bezeichnen wir mit Q.

Dann folgt aus (17[b]) und aus unserer Formel für $\chi(p^\alpha) : \chi(p^{\alpha-1})$

$$\begin{aligned}
\chi(p^{\alpha_1}) &= p^Q, \\
\chi(p^{\alpha_1-1}) &= p^{Q - q_{\alpha_1}}, \\
\chi(p^{\alpha_1-2}) &= p^{Q - q_{\alpha_1} - 1 - 2q_{\alpha_1}}, \\
\chi(p^{\alpha_1-3}) &= p^{Q - q_{\alpha_1} - 2 - 2q_{\alpha_1} - 1 - 3q_{\alpha_1}}, \\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

§ 513. Mit Hülfe der bisher gefundenen Resultate können wir jetzt den schon oben (§ 509, Schluss) angedeuteten Satz beweisen, dass die Anzahl sowie der Werth der einzelnen Invarianten $n_1, n_2, \cdots n_r$ einer Abel'schen Gruppe $\mathfrak{A}$ von der Wahl der Basis dieser Gruppe unabhängig sind.

Von der ersten Invariante n_1 ist dies ja ihrer Bedeutung nach von selbst klar, da nach H) § 509 n_1 die kleinste Zahl ist, welche die sämmtlichen Exponenten, zu denen die Elemente von $\mathfrak{A}$ gehören, zu Theilern hat. Dagegen ist das Element Θ_1 nicht eindeutig bestimmbar, und von der Wahl dieses Θ_1 könnte möglicherweise n_2 abhängen, u. s. f.

Den Beweis des aufgestellten Theorems führen wir folgendermassen.

Aus der Bedeutung von (17) und (17[a]) als Anzahl von Elementen der Gruppe $\mathfrak{A}$, welche eine ganz bestimmt definirte Eigenschaft haben, folgt, dass der Werth (17) von der Wahl der Basis unabhängig ist. Schreibt man nun (17) in der Gestalt

$$p^{(\alpha-1)\varkappa + \alpha_{\varkappa+1} + \cdots + \alpha_r}(p^\varkappa - 1),$$

so erkennt man, dass $(p^{\varkappa} - 1)$ eindeutig durch den Werth von (17) gegeben ist, nämlich als der durch p nicht theilbare Factor dieser Zahl, und daraus, dass auch $\varkappa$ unabhängig von der Basis bestimmt ist. Die Zahl der durch ein p^{α} theilbaren Glieder der zu den Elementen irgend einer Basis gehörigen Exponenten

$$(18^{a}) \qquad n_1, \; n_2, \; n_3, \; \cdots \; n_r$$

ist von der Wahl der Basis unabhängig. Sind nun mindestens die ersten ϱ Glieder von (18ª) durch p^{α} theilbar, dagegen weniger als ϱ der ersten Glieder durch $p^{\alpha+1}$, dann ist n_{ϱ} genau durch p^{α} theilbar. Die höchste Potenz von p, welche ein seiner Stellung nach gegebenes Glied aus (18ª) theilt, ist von der Wahl der Basis unabhängig. Führt man die Bestimmung dieser höchsten Primzahlpotenz in n_{ϱ} für alle Primfactoren von n, oder, was dasselbe besagt, von n_1 durch, dann folgt, dass der Werth von n_{ϱ} selbst von der Wahl der Basis unabhängig sei; und damit ist der aufgestellte Satz bewiesen.

Insbesondere ist auch die Zahl r nur von der Gruppe, nicht von ihrer Basis abhängig. Wir wollen diese Zahl r als den Rang der Abel'schen Gruppe bezeichnen. Auch der Rang der Gruppe ist invariant. Eine Abel'sche Gruppe vom Range 1 heisst eine cyklische Gruppe. Alle ihre Elemente können als Potenzen ein und desselben Elementes dargestellt werden.

§ 514. Es möge eine Abel'sche Gruppe $\mathfrak{A}$ die Elemente Θ_1, $\Theta_2, \cdots \Theta_n$ umfassen; dies wollen wir durch

$$\mathfrak{A} = [\Theta_1, \Theta_2, \cdots \Theta_n]$$

kurz ausdrücken, wobei also die eckige Klammer sämmtliche Elemente von $\mathfrak{A}$ einschliessen soll. Ferner sei $n = h \cdot k$, und es soll möglich sein, aus der Gruppe $\mathfrak{A}$ zwei Theiler $\mathfrak{A}_1$ und $\mathfrak{A}_2$ herauszuheben

$$\mathfrak{A}_1 = [\vartheta_1, \vartheta_2, \cdots \vartheta_h], \quad \mathfrak{A}_2 = [\tau_1, \tau_2, \cdots \tau_k]$$

von der Art, dass jedes Θ als Product $\vartheta_{\alpha} \cdot \tau_{\beta}$ $(\alpha = 1, 2, \cdots h; \; \beta = 1, 2, \cdots k)$ dargestellt werden kann. Dann sagen wir, $\mathfrak{A}$ sei aus $\mathfrak{A}_1$ und $\mathfrak{A}_2$ componirt, oder $\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{A}_2$ sei das Product von $\mathfrak{A}_1$ und $\mathfrak{A}_2$. — $\mathfrak{A}$ heisst in diesem Falle zerlegbar. Hierbei muss bemerkt werden, dass die Existenz eines Theilers $\mathfrak{A}_1$ von $\mathfrak{A}$ durchaus nicht die Zerlegbarkeit der Gruppe $\mathfrak{A}$ nach sich zu ziehen braucht.

Da $\mathfrak{A}_1$ und $\mathfrak{A}_2$ Gruppen sind, so hat jede das Einheitselement E von $\mathfrak{A}$ unter ihren Elementen. Den gemachten Annahmen gemäss ist dies das einzige gemeinsame Element beider Gruppen. Denn alle $\vartheta_{\alpha} \tau_{\beta}$ müssen bei den $h \cdot k$ verschiedenen Indexsystemen α, β verschieden

ausfallen. Wäre aber ein von E verschienes ϑ_0 gleich einem τ_0, so würde das formal von $\vartheta_\alpha \tau_\beta$ verschiedene Product

$$(\vartheta_\alpha \vartheta_0)(\tau_0^{-1} \tau_\beta) = \vartheta_\alpha \tau_\beta$$

gegen die Voraussetzung werden, und es wären also nicht alle $h \cdot k = n$ Producte unter einander verschieden.

Es ist klar, dass durch die Formel (8), § 509 die Zerlegung einer Abel'schen Gruppe vom Range r in r Factoren vom Range 1, d. h. in r cyklische Gruppen geliefert wird. Sobald also $r > 1$ ist, ist eine Zerlegung der Gruppe $\mathfrak{A}$ möglich.

Hiermit ist jedoch die Frage nach der Zerlegbarkeit einer Abel-schen Gruppe noch nicht zu Ende geführt; es ist zur Ergänzung die Entscheidung darüber herbeizuführen, wann und wie auch eine cyklische Gruppe

$$\mathfrak{A} = [\Theta, \Theta^2, \Theta^3, \cdots, \Theta^n] \qquad (\Theta^n = E)$$

zerlegt werden kann. Gesetzt es gäbe zwei solche Factoren $\mathfrak{A}_1$ und $\mathfrak{A}_2$ von den Ordnungen h und k, wie sie oben angedeutet sind, dann müsste es in $\mathfrak{A}_1$ ein Element ϑ und in $\mathfrak{A}_2$ ein τ derart geben, dass $\vartheta \tau = \Theta$ wird. Da nun die Elemente ϑ und τ vertauschbar sind, so folgt

$$\vartheta \tau = \Theta, \quad \vartheta^2 \tau^2 = \Theta^2, \quad \vartheta^3 \tau^3 = \Theta^3, \quad \cdots \quad \vartheta^n \tau^n = \Theta^n = E,$$

und hierdurch werden alle Elemente der Gruppe $\mathfrak{A}$ festgelegt. Von diesen betrachten wir

$$\vartheta^k \tau^k, \quad \vartheta^{2k} \tau^{2k}, \quad \vartheta^{3k} \tau^{3k}, \quad \cdots \quad \vartheta^{hk} \tau^{hk} = E.$$

Da τ zu einer Gruppe von der Ordnung k gehört, so ist gemäss § 508, E) zu setzen $\tau^k = E$, und also gehören

$$\vartheta^k, \quad \vartheta^{2k}, \quad \cdots \quad \vartheta^{hk} = E$$

zu $\mathfrak{A}_1$. Sie sind ferner von einander verschieden, weil sie bezw. gleich Θ^k, Θ^{2k}, $\cdots$ sind; folglich bildet ihre Gesammtheit die Abel'sche Gruppe $\mathfrak{A}_1$, d. h. es ist

$$\mathfrak{A}_1 = [\vartheta^k, \vartheta^{2k}, \cdots \vartheta^{hk}].$$

Ferner ist jede Substitution von $\mathfrak{A}_1$ so beschaffen, dass ihre h^{te} Potenz gleich E wird, da die Ordnung von $\mathfrak{A}_1$ gleich h ist; § 508, E). Deshalb kann aus der Reihe $k, 2k, \cdots hk$ der eben benutzten Exponenten nur der letzte durch h theilbar werden, d. h. h und k sind theilerfremd zu einander.

Ebenso erkennt man, dass

$$\mathfrak{A}_2 = [\tau^h, \tau^{2h}, \cdots \tau^{kh}]$$

ist; ferner kann man beide Gruppen in die Formen bringen

$$\mathfrak{A}_1 = [\Theta^k, \Theta^{2k}, \cdots \Theta^{hk}], \quad \mathfrak{A}_2 = [\Theta^h, \Theta^{2h}, \cdots \Theta^{kh}].$$

Umgekehrt ist klar, dass, wenn durch $n = k \cdot h$ die Zahl n in zwei theilerfremde Factoren h und k zerlegt worden ist, die Zerlegung $\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{A}_2$ gilt, weil man ganzzahlig x und y so bestimmen kann, dass

$$\Theta^{kx+hy} = \Theta$$

wird. So zeigt es sich: Eine cyklische Gruppe $\mathfrak{A}$ kann dann und nur dann zerlegt werden, wenn ihre Ordnung n in zwei theilerfremde Factoren h, k zerfällt werden kann. — Nur cyklische Gruppen, deren Ordnung eine Primzahlpotenz ist, sind unzerlegbar.

§ 515. Es fragt sich nun, ob diese Zerlegung einer Gruppe in unzerlegbare Factoren auf mehrfache oder nur eine einzige Art vor sich gehen kann; und falls die erste Möglichkeit eintreten sollte, ob es gewisse, für alle vorhandenen Zerlegungen invariante Beziehungen giebt. Das soll jetzt untersucht werden.

Wir gehen auf die erste der Formeln (17^b) zurück und beachten, dass der Exponent von p in

$$(17^b) \qquad \chi(p^{\alpha_1}) = p^{\alpha_1 + \alpha_2 + \cdots + \alpha_r}$$

die höchste Potenz der Primzahl p ist, welche $n_1 \cdot n_2 \cdots n_r$, d. h. die Ordnung n von $\mathfrak{A}$ theilt. (17^b) giebt die Anzahl aller Elemente Θ von $\mathfrak{A}$, welche der Gleichung

$$\Theta^{p^{\alpha_1}} = E$$

genügen. Da $\alpha_1 \leqq \alpha_1 + \alpha_2 + \cdots$, so folgt: Ist p^α die höchste Potenz von p, welche die Ordnung n von $\mathfrak{A}$ theilt, dann giebt es genau p^α Elemente in $\mathfrak{A}$, deren Ordnung eine Potenz von p ist.

Weiter erkennt man sofort, wenn man ebenso eine zweite, dritte, $\cdots$ Primzahlpotenz betrachtet: Ist $n = g \cdot h$, wo g und h theilerfremd sind, dann giebt es in $\mathfrak{A}$ genau g Elemente, welche der Gleichung genügen

$$\Theta^g = E.$$

Hat man also $\mathfrak{A}$ in zwei Factoren $\mathfrak{A}_1$, $\mathfrak{A}_2$ zerlegt, so dass g die Ordnung von $\mathfrak{A}_1$ und h diejenige von $\mathfrak{A}_2$ ist, dann kann bei theilerfremden g, h diese Zerlegung nur auf eine Art vor sich gehen, da

eben $\mathfrak{A}_1$ nur die eindeutig bestimmten g Elemente enthalten kann, welche durch die letzte Gleichung bestimmt sind, und da für $\mathfrak{A}_2$ und h Aehnliches gilt.

Dies zeigt uns: Die Zerlegung einer Abel'schen Gruppe in Theiler, deren Ordnungen Primzahlpotenzen sind, ist nur auf eine einzige Art möglich. Unsere Frage ist also auf diejenige nach der Zerfällung solcher Gruppen reducirt.

Wir betrachten demnach jetzt eine Abel'sche Gruppe $\mathfrak{A}$ der Ordnung p^a. Es seien $\Theta_1, \Theta_2, \cdots$ die Elemente einer Basis der Gruppe und

$$p^{\alpha_1},\ p^{\alpha_2}, \cdots \qquad (\alpha_1+\alpha_2+\cdots=a;\ \alpha_1\geqq\alpha_2\geqq\cdots)$$

die zugehörigen Invarianten, die ja gleichfalls Potenzen von p sein müssen. Ferner sei

$$\mathfrak{A}=\mathfrak{A}_1\cdot\mathfrak{A}_2\cdots\mathfrak{A}_\varrho,$$

so dass $\mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_\varrho$ unzerlegbare Gruppen sind, also solche vom Range 1 und von einer Primzahlpotenz-Ordnung q_1, bezw. $q_2, \cdots q_\varrho$; dabei möge $q_1 \geqq q_2 \geqq \cdots \geqq q_\varrho$ sein. Dann sind $\mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_\varrho$ durch die Potenzen gewisser Elemente $\vartheta_1, \vartheta_2, \cdots \vartheta_\varrho$ gebildet, und $\mathfrak{A}$ besteht aus allen

$$\vartheta_1^{\mu_1}\vartheta_2^{\mu_2}\cdots\vartheta_\varrho^{\mu_\varrho} \qquad (\mu_\alpha=0,1,\cdots q_\alpha-1). \tag{19}$$

Die q_α sind sämmtlich Potenzen von p, und q_1 wird die höchste vorkommende Ordnung eines Elementes von $\mathfrak{A}$ und also deswegen gleich der ersten Invariante $q_1=p^{\alpha_1}$.

Ferner zeigt die Form (19) der Elemente von $\mathfrak{A}$, dass jedes Element in die q_2^{te} Potenz erhoben gleich einer Potenz von ϑ_1 wird, und dass q_2 die niedrigste derartige Zahl wird. Folglich ist q_2 die zweite Invariante und also gleich p^{α_2}.

In dieser Art kann man fortfahren und erkennt, dass $\mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_\varrho$ durch $\vartheta_1, \vartheta_2, \cdots \vartheta_\varrho$ eine Basis von $\mathfrak{A}$ liefern, und dass

$$q_1=p^{\alpha_1},\quad q_2=p^{\alpha_2},\quad \cdots \quad q_\varrho=p^{\alpha_\varrho}$$

wird. Ist die Zerlegung einer Abel'schen Gruppe von Primzahlpotenz-Ordnung auf mehrere Arten durchführbar, so ist die Anzahl der irreductiblen Factoren stets dieselbe, und eine solche Zuordnung der einen und der anderen Factoren zu einander möglich, dass entsprechende Factoren gleiche Ordnungen haben. Dass wirklich verschiedene Zerfällungen eintreten können, erkennt man leicht. Es sei $\tau_1^2=1$, $\vartheta_1^2=1$ und

$$\mathfrak{A}=[E,\ \tau_1,\ \vartheta_1,\ \tau_1\vartheta_1];$$

dann kann man für $\mathfrak{A}_1 \cdot \mathfrak{A}_2 = \mathfrak{A}$

$$\mathfrak{A}_1 = [E, \tau_1], \qquad \mathfrak{A}_2 = [E, \vartheta_1],$$

aber ebensogut auch

$$\mathfrak{A}_1 = [E, \tau_1 \vartheta_1], \quad \mathfrak{A}_2 = [E, \tau_1]$$

oder

$$\mathfrak{A}_1 = [E, \tau_1 \vartheta_1], \quad \mathfrak{A}_2 = [E, \vartheta_1]$$

setzen.

Es ist also bewiesen: Wie auch eine Abel'sche Gruppe in irreductible Factoren zerlegt wird, die Ordnungen dieser Factoren und ihre Anzahlen haben stets dieselben Werthe.

§ 516. Es möge nun

$$\mathfrak{A}_1 = [\Theta', \Theta'', \cdots \Theta^{(h)}]$$

ein beliebiger Theiler der Ordnung h von $\mathfrak{A}$ mit der Ordnung $n = h \cdot k$ sein. Dabei wollen wir nochmals bemerken, dass dann $\mathfrak{A}$ nicht nothwendiger Weise in Factoren sich zerfällen lässt, deren einer gleich $\mathfrak{A}_1$ ist. Wir bilden eine symmetrische Function der Elemente von $\mathfrak{A}_1$, welche wir bezeichnen wollen

$$S(\Theta', \Theta'', \cdots \Theta^{(h)}) = \varphi.$$

Ist Θ_α ein Element von $\mathfrak{A}$, welches nicht in $\mathfrak{A}_1$ vorkommt, so sind auch die Producte

$$\Theta_\alpha \Theta', \;\; \Theta_\alpha \Theta'', \;\cdots\; \Theta_\alpha \Theta^{(h)}$$

sämmtlich in $\mathfrak{A}$ enthalten und sie sind unter sich und von den Elementen von $\mathfrak{A}_1$ verschieden (§ 509, J); wir bilden mit diesen neuen Elementen als Argumenten die entsprechende Function

$$S(\Theta_\alpha \Theta', \Theta_\alpha \Theta'', \cdots \Theta_\alpha \Theta^{(h)}) = \varphi_\alpha$$

und fahren so fort, wenn Θ_β ein neues Element bezeichnet,

$$S(\Theta_\beta \Theta', \Theta_\beta \Theta'', \cdots \Theta_\beta \Theta^{(h)}) = \varphi_\beta,$$

$$\cdots\cdots\cdots\cdots\cdots$$

So entstehen k Werthe $\varphi, \varphi_\alpha, \varphi_\beta, \cdots$, die wir als Elemente einer neuen Art auffassen, und zwischen denen wir folgendes Compositionsgesetz feststellen wollen.

Es sei φ_γ durch die Composition von φ_α und φ_β entstanden, d. h.

$$\varphi_\alpha \varphi_\beta = \varphi_\gamma, \quad \text{wenn} \quad [\Theta_\alpha \Theta^{(\varkappa)}] \cdot [\Theta_\beta \Theta^{(\lambda)}] = \Theta_\gamma \Theta^{(\mu)}$$

ist; das γ ist dabei von der Wahl von $\varkappa$ und λ unabhängig, oder vielmehr: die ganze Zeile, welche Θ_α enthält, mit der von Θ_β componirt, giebt eine bestimmte dritte Zeile. Es ist also die Composition

eine eindeutig durch die Factoren bestimmte (§ 507, I). Ferner gilt das associative Gesetz (§ 507, II), d. h. es ist

$$[\varphi_\alpha \varphi_\beta]\varphi_\gamma = \varphi_\alpha[\varphi_\beta \varphi_\gamma],$$

weil

$$([\Theta_\alpha \Theta^{(\varkappa)}][\Theta_\beta \Theta^{(\lambda)}]) \cdot [\Theta_\gamma \Theta^{(\mu)}] = [\Theta_\alpha \Theta^{(\varkappa)}] \cdot ([\Theta_\beta \Theta^{(\lambda)}][\Theta_\gamma \Theta^{(\mu)}])$$

ist. Ebenso zeigt man, dass wie § 507, III) es fordert, aus

$$\varphi_\alpha \varphi_\beta = \varphi_\alpha \varphi_\gamma \quad \text{folgt} \quad \varphi_\beta = \varphi_\gamma;$$

und dass endlich entsprechend § 509, IV) auch

$$\varphi_\alpha \varphi_\beta = \varphi_\beta \varphi_\alpha$$

wird. Die symmetrischen Functionen $\varphi, \varphi_\alpha, \varphi_\beta, \cdots$ bilden demnach die Elemente einer Abel'schen Gruppe.

§ 517. Wir wollen von den in dieser Vorlesung bisher abgeleiteten Resultaten nun die Anwendung auf Abel'sche Gleichungen machen und zu diesem Zwecke zunächst nachweisen, dass die Wurzeln einer jeden Abel'schen Gleichung als die Elemente einer Abel'schen Gruppe aufgefasst werden können.

Nach der Definition aus § 503 ist es möglich, alle Wurzeln einer Abel'schen Gleichung $f(z) = 0$ rational durch eine von ihnen auszudrücken. Wir wollen diese z' nennen und setzen aus Gründen, die wir sofort erkennen werden,

$$z' = E(z');$$

das Symbol E betrachten wir dabei als Einheitssymbol oder Einheitselement. Die weiteren Wurzeln der Gleichung mögen, als Functionen von z' dargestellt,

$$\Theta'(z'),\ \Theta''(z'),\ \Theta'''(z'),\ \cdots$$

sein. Bei ihnen wie bei $E(z')$ unterdrücken wir das Argument und schreiben

$$E,\ \Theta',\ \Theta'',\ \Theta''',\ \cdots.$$

Diese Symbole fassen wir als Elemente auf und definiren ihre Composition durch die Gleichung

$$\Theta'\Theta'' = \Theta'[\Theta''(z')] = \Theta'''(z') = \Theta'''.$$

Aus der Definition der Abel'schen Gleichungen folgt dann die Eindeutigkeit der Composition, sowie auch die Gültigkeit des associativen und des commutativen Gesetzes. Ist ferner $\Theta'^{-1}(z')$ diejenige Wurzel, die mit $\Theta'(z')$ componirt $E(z') = z'$ ergiebt, und deren Existenz aus der Reihe

$$\Theta',\ \Theta'(\Theta'),\ \Theta'[\Theta'(\Theta')],\ \cdots$$

zu entnehmen ist, so folgt aus der Richtigkeit einer Gleichung von der Form

$$\Theta'[\Theta''(z')] = \Theta'[\Theta'''(z')]$$

durch linksseitige Composition mit Θ'^{-1}, dass $\Theta'' = \Theta'''$ wird. Damit sind alle Bedingungen als erfüllt nachgewiesen, welche sich auf Abel'sche Gruppen beziehen, und es folgt, dass die Wurzeln jeder Abel'schen Gleichung als Elemente einer Abel'schen Gruppe angesehen werden können.

Nun sind wir auch im Stande, unsere Methode und unsere Resultate aus § 504 zu erweitern. Bilden

$$(20) \qquad \vartheta_1, \vartheta_2, \vartheta_3, \cdots \vartheta_h$$

einen Theil der Wurzeln der vorgelegten Abel'schen Gleichung, welchem auch die Gruppeneigenschaft zukommt, dann ist erstens

$$(21) \qquad (z - \vartheta_1)(z - \vartheta_2) \cdots (z - \vartheta_h) = 0$$

eine Abel'sche Gleichung h^{ten} Grades, und die k Werthe jeder symmetrischen Function, welche innerhalb der vorgelegten Abel'schen Gleichung auftreten,

$$\varphi = S(\vartheta_1, \vartheta_2, \cdots \vartheta_h) \qquad (h \cdot k = n)$$

sind nach dem vorigen Paragraphen gleichfalls als Wurzeln einer Abel'schen Gleichung k^{ten} Grades anzusehen, sobald feststeht, dass sie sämmtlich rationale Functionen von φ sind. Das wird aber genau so bewiesen, wie der entsprechende Satz aus § 505. Ist demnach (20) ein Theiler h^{ter} Ordnung der zu $f(z) = 0$ gehörigen Abel'schen Gruppe, dann kann die Lösung der Gleichung $f(z) = 0$ auf diejenige einer Abel'schen Gleichung h^{ten} und einer solchen k^{ten} Grades zurückgeführt werden, deren erstere die Gleichung (21) ist. Ihre Coefficienten werden durch die Lösung der zweiten Gleichung vom k^{ten} Grade rational bekannt.

Aus den Untersuchungen über die Abel'schen Gruppen sind wir ferner in die Lage gesetzt, die Lösung von $f(z) = 0$ in ihre einfachsten Bestandtheile zu zerspalten und diese als invariant nachzuweisen.

Zu diesem Behufe zerlegen wir den Grad n der Gleichung, welche zugleich die Ordnung der zugehörigen Abel'schen Gruppe angiebt, in seine Basis-Invarianten

$$(10) \qquad n = n_1 \cdot n_2 \cdot \cdots n_r;$$

die zu den einzelnen Invarianten gehörigen Elemente mögen

$$\Theta_1, \Theta_2, \cdots \Theta_r$$

heissen; dann ist die Gruppe in die cyklischen Gruppen

$$\Theta_\varkappa^{\alpha_\varkappa} \qquad (\varkappa = 1, 2, \cdots r;\ \alpha_\varkappa = 1, 2, \cdots n_\varkappa)$$

zerlegbar. Ist ein $n_\varkappa$ eine aus verschiedenen Primzahlen zusammengesetzte Zahl, so kann die Zerlegung der Gruppen in unzerlegbare Factoren noch fortgesetzt werden. So entsteht eine Reihe einfachster Gruppen, deren Ordnungen Primzahlpotenzen sind,

$$p_1^{\varrho_1},\ p_2^{\varrho_2},\ p_3^{\varrho_3}, \cdots; \qquad \left(n = p_1^{\varrho_1} \cdot p_2^{\varrho_2} \cdot p_3^{\varrho_3} \cdots\right),$$

es können unter den Primzahlen p_1, p_2, $\cdots$ auch gleiche vorkommen. Nimmt man dann als Hülfsgleichungen der Reihe nach eine solche des Grades $p_1^{\varrho_1}$, des Grades $p_2^{\varrho_2}$, $\cdots$, dann ist durch deren Lösung die Lösung von $f(z) = 0$ vollbracht. Die Anordnung dieser Hülfsgleichungen ist dabei ganz beliebig. Die Invarianz ihrer Grade folgt aus § 515. Hiermit ist eine wichtige Ergänzung zu unseren früheren Untersuchungen geliefert, bei denen noch nicht bewiesen war, dass nicht durch Aenderung der Operationenfolge auch die Grade der auflösenden Hülfsgleichungen einer Aenderung unterworfen werden könnten.

Zweiundfünfzigste Vorlesung.

Alternirende und cyklische Functionen. Anwendung auf Abel'sche Gleichungen.

§ 518. Um die Abel'schen Gleichungen noch von einer anderen Seite her zu betrachten, haben wir jetzt eine gewisse Art von Functionen von n Veränderlichen zu untersuchen, die eine ähnlich wichtige Rolle spielen, wie die symmetrischen Functionen. Es wird aber gut sein, hier gleich weiter auszuholen, um diesen Functionen ihre richtige Stelle anzuweisen und um den Boden für künftige Untersuchungen vorzubereiten. Wir wollen dazu direct an die symmetrischen Functionen anknüpfen.

In der neunten Vorlesung (Bd. I) haben wir eingehend die Haupteigenschaften der symmetrischen Functionen von n Grössen z_1, z_2, $\cdots$ z_n behandelt, welche als unbestimmte Grössen angenommen wurden; es sind dies diejenigen Functionen, welche ihre Form bei jeder möglichen Umstellung der z untereinander beibehalten. Wir können sie dieser Eigenschaft halber auch als einwerthige Functionen bezeichnen. Alle rationalen ganzen, symmetrischen Functionen der z_α wollen wir in eine Gattung vereinigt denken.

Fassen wir die einzelnen Vertauschungen der z untereinander als Elemente im Sinne der vorigen Vorlesung auf, dann zeigt es sich, dass ihre Gesammtheit eine Gruppe bildet.

Wir bezeichnen die **Vertauschung** oder die **Substitution**, welche die Elemente $z_1, z_2, \cdots z_n$ in eine andere Anordnung $z_{i_1}, z_{i_2}, \cdots z_{i_n}$ überführt, wobei $i_1, i_2, \cdots i_n$ also irgend eine der $n!$ Permutationen der Zahlen $1, 2, \cdots n$ bedeutet, durch das Symbol

$$(1) \qquad s_i = \begin{pmatrix} z_1 & z_2 & \cdots & z_n \\ z_{i_1} & z_{i_2} & \cdots & z_{i_n} \end{pmatrix},$$

oder auch wohl kürzer, falls keine Zweideutigkeit entsteht, durch

$$(1^a) \qquad s_i = \begin{pmatrix} z_\alpha \\ z_{i_\alpha} \end{pmatrix} = \begin{pmatrix} \alpha \\ i_\alpha \end{pmatrix}.$$

Als Einheitselement nehmen wir die durch $i_1 = 1, i_2 = 2, \cdots i_n = n$ bestimmte identische Substitution

$$s = \begin{pmatrix} \alpha \\ \alpha \end{pmatrix} = 1,$$

deren Existenz ja klar ist.

Ferner definiren wir als Composionsresultat oder als „**Product**“ von s_i, s_k diejenige Umstellung, welche entsteht, wenn man auf die durch s_i hervorgerufene Umstellung s_k anwendet; so entsteht das eindeutig bestimmte durch „**Multiplication**“ gebildete Product

$$(2) \qquad s_i s_k = \begin{pmatrix} z_\alpha \\ z_{i_\alpha} \end{pmatrix} \begin{pmatrix} z_\alpha \\ z_{k_\alpha} \end{pmatrix} = \begin{pmatrix} z_\alpha \\ z_{i_\alpha} \end{pmatrix} \begin{pmatrix} z_{i_\alpha} \\ z_{k_{i_\alpha}} \end{pmatrix} = \begin{pmatrix} z_\alpha \\ z_{k_{i_\alpha}} \end{pmatrix} = \begin{pmatrix} \alpha \\ k_{i_\alpha} \end{pmatrix}.$$

Aus (2) folgt das associative Gesetz für irgend welche drei Substitutionen s_i, s_k, s_l; denn man hat

$$(s_i s_k) s_l = \begin{pmatrix} \alpha \\ k_{i_\alpha} \end{pmatrix} \begin{pmatrix} \alpha \\ l_\alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ l_{k_{i_\alpha}} \end{pmatrix},$$

$$s_i (s_k s_l) = \begin{pmatrix} \alpha \\ i_\alpha \end{pmatrix} \begin{pmatrix} \alpha \\ l_{k_\alpha} \end{pmatrix} = \begin{pmatrix} \alpha \\ l_{k_{i_\alpha}} \end{pmatrix}.$$

Ist weiter $s_i s_k = s_i s_\varkappa$, so ergiebt sich sofort aus (2)

$$k_{i_\alpha} = \varkappa_{i_\alpha} \quad \text{d. h.} \quad k_\beta = \varkappa_\beta \qquad (\beta = 1, 2, \cdots n)$$

und daher $s_k = s_\varkappa$. — Und ebenso liefert die Annahme $s_k s_i = s_\varkappa s_i$ wegen (2)

$$i_{k_\alpha} = i_{\varkappa_\alpha} \quad \text{d. h.} \quad k_\alpha = \varkappa_\alpha \qquad (\alpha = 1, 2, \cdots n)$$

und deshalb $s_k = s_\varkappa$.

Greift man daher aus der Gesammtheit der $n!$ Substitutionen einen Complex von der Eigenschaft heraus, dass das Product zweier Elemente desselben wiederum zu dem Complexe gehört, dann gelten die Bedingungen I, II, III des § 507, und dadurch ist der Complex als Gruppe erkannt; wir nennen sie Substitutionengruppe.

Die Rolle der Einheit E übernimmt hier die identische Substitution

$$1 = \binom{z_\alpha}{z_\alpha} = \binom{\alpha}{\alpha}\cdot$$

Genau wie in § 508, B weist man auch hier nach, dass für jedes in der Gruppe enthaltene s_i ein Element besteht, mit dem s_i componirt die Einheit ergiebt. Wir bezeichnen es mit s_i^{-1} und haben

$$s_i \cdot s_i^{-1} = 1, \quad s_i^{-1} \cdot s_i = 1.$$

Es ist $(s_i s_t)^{-1} = s_t^{-1} s_i^{-1}$, wie man erkennt, wenn man beide Seiten rechts oder links mit $s_i s_t$ multiplicirt.

Die Bildung von Potenzen einer Substitution, die Ordnung einer solchen, der Begriff des Divisors oder Theilers einer Gruppe sind direct aus § 508 zu entnehmen.

Die Gesammtheit aller Substitutionen als Gruppe betrachtet nennen wir die symmetrische Substitutionengruppe.

§ 519. Im § 121 der zehnten Vorlesung (Bd. I) lernten wir eine Function

$$(3) \quad \varphi_1 = \prod_{\lambda, \mu} (z_\lambda - z_\mu), \qquad (\lambda = 1, 2, \cdots n-1;\ \mu = \lambda + 1, \cdots n)$$

kennen, welche bei allen Substitutionen der symmetrischen Gruppe zwei und nur zwei Werthe, φ_1 und $\varphi_2 = -\varphi_1$ annimmt. Wir wollen jede rationale Function der z, welche unter der Einwirkung der $n!$ verschiedenen Substitutionen zwei, nur durch ihr Vorzeichen verschiedene Werthe annimmt, eine alternirende Function nennen und zunächst sämmtliche ganzen, alternirenden Functionen aufsuchen.

Bei (3) haben wir gesehen, dass durch die Vertauschung zweier Elemente z untereinander eine Werthänderung von φ_1 herbeigeführt wird. Eine solche Vertauschung, etwa von z_α und z_β, schreiben wir $(z_\alpha z_\beta)$ oder $(z_\beta z_\alpha)$ und nennen diese specielle Substitution eine Transposition.

Jede Substitution der n Elemente $z_1, \cdots z_n$ kann durch ein Product von höchstens $(n-1)$ Transpositionen ersetzt werden. Denn es ist, wenn s_i die geforderte Substitution bedeutet,

$$\begin{pmatrix} z_1 & z_2 & \cdots & z_{i_1} & \cdots & z_n \\ z_{i_1} & z_{i_2} & \cdots & z_{i_{i_1}} & \cdots & z_{i_n} \end{pmatrix} = (z_1 z_{i_1}) \begin{pmatrix} z_{i_1} & z_2 & \cdots & z_1 & \cdots & z_n \\ z_{i_1} & z_{i_2} & \cdots & z_{i_{i_1}} & \cdots & z_{i_n} \end{pmatrix},$$

so dass nach Ausführung der Transposition $(z_1 z_{i_1})$ nur noch die Substitution, bei welcher das z_{i_1} der oberen Zeile ungeändert bleibt,

$$\begin{pmatrix} z_{i_1} & z_2 & \cdots & z_1 & \cdots & z_n \\ z_{i_1} & z_{i_2} & \cdots & z_{i_{i_1}} & \cdots & z_{i_n} \end{pmatrix} \quad \text{d. h.} \quad \begin{pmatrix} z_2 & \cdots & z_1 & \cdots & z_n \\ z_{i_2} & \cdots & z_{i_{i_1}} & \cdots & z_{i_n} \end{pmatrix}$$

zu bewerkstelligen ist. Ihre letzte Form zeigt, dass wir dabei von z_{i_1} absehen können und es dann lediglich mit einer Substitution von $(n-1)$ Elementen z zu thun haben. Gehen wir in derselben Art von ihr aus weiter, so gelangen wir nach $(n-2)$ Schritten zu einer Substitution von zwei Variablen, für welche der Satz dann selbstverständlich ist.

Daraus folgt: Eine Function, welche bei allen Transpositionen ungeändert bleibt, ist eine symmetrische Function. Denn sie bleibt gemäss der Voraussetzung und nach dem vorigen Satze für jede Substitution ungeändert.

Die Zerfällung einer Substitution in Transpositionen kann auf mannigfache Arten vor sich gehen. So lässt sich z. B. die identische Substitution durch jede der Folgen von Transpositionen

$$(z_1 z_2)(z_1 z_3)(z_2 z_3)(z_1 z_3), \quad (z_1 z_2)(z_3 z_4)(z_2 z_4)(z_1 z_3)(z_1 z_4)(z_2 z_3),$$
$$(z_1 z_2)(z_3 z_4)(z_1 z_5)(z_2 z_4)(z_1 z_3)(z_2 z_3)(z_2 z_5)(z_1 z_4), \cdots$$

darstellen.

Die gesuchten ganzen, alternirenden Functionen ψ müssen mindestens für eine Transposition, etwa für $(z_\alpha z_\beta)$, ihr Vorzeichen ändern. Dies können wir durch die Gleichung

$$\psi(z_1, \cdots, z_\alpha, \cdots, z_\beta, \cdots, z_n) = -\psi(z_1, \cdots, z_\beta, \cdots, z_\alpha, \cdots, z_n)$$

darstellen. Hieraus ergiebt sich, dass jedem Potenzproducte

$$c z_1^{m_1} \cdots z_\alpha^p \cdots z_\beta^q \cdots z_n^{m_n}$$

des Polynoms ψ ein in ψ gleichfalls vorhandenes Potenzproduct

$$-c z_1^{m_1} \cdots z_\alpha^q \cdots z_\beta^p \cdots z_n^{m_n}$$

entspricht; und aus der Vereinigung je zweier so gestalteter erkennt man, dass ψ durch $(z_\alpha - z_\beta)$ theilbar ist. Die Function ψ^2 ist offenbar symmetrisch, und da sie den Factor $(z_\alpha - z_\beta)^2$ enthält, so ist sie durch die Discriminante theilbar. Diese wollen wir, von dem in § 158, Bd. I festgesetzten Vorzeichen absehend,

$$D = \prod_{\lambda, \mu} (z_\lambda - z_\mu)^2 \qquad (\lambda = 1, 2, \cdots n-1;\ \mu = \lambda + 1, \cdots n)$$

schreiben. D selbst ist einwerthig, $\sqrt{D}$ ist alternirend. Bedeutet

jetzt $(\sqrt{D})^k$ die höchste Potenz von $\sqrt{D}$, welche in ψ als Factor enthalten ist,

$$\psi = \psi' \cdot (\sqrt{D})^k,$$

so würde bei geradem k der Factor ψ' noch alternirend sein und müsste deshalb wieder $\sqrt{D}$ als Factor haben. Dies ist ausgeschlossen, und folglich muss k ungerade $= 2\varkappa + 1$, und

$$\psi' = \frac{\psi}{(\sqrt{D})^{2\varkappa+1}}$$

sein. Die rechte Seite wird hier nicht alternirend; denn sonst wäre ja ψ' noch durch $\sqrt{D}$ theilbar; sie ist also einwerthig. Wenn demnach S_1 eine beliebige ganze, symmetrische Function von $z_1, z_2, \cdots z_n$ bezeichnet, dann können wir allgemein

$$\psi(z_1, \cdots z_n) = S_1 \cdot \sqrt{D} \tag{4}$$

setzen, da $(\sqrt{D})^{2\varkappa}$ ja selbst symmetrisch ist. Der Ausdruck (4) giebt jede ganze, alternirende Function der Elemente z_1, $z_2, \cdots z_n$.

§ 520. Aus § 121, Bd. I kann man entnehmen, dass $\sqrt{D}$ und damit jede alternirende Function unter dem Einflusse jeder Transposition ihr Zeichen ändert; denn was dort von z_1 und z_2 gesagt war, gilt für jedes z_α und jedes z_β. Dieser Umstand zeigt uns, dass die Anwendung einer geraden Anzahl von Transpositionen nach einander den Werth von ψ nicht ändert, während bei der Anwendung einer ungeraden Anzahl das Vorzeichen von ψ in das entgegengesetzte übergeht. Hieraus kann man weiter entnehmen, dass, wenn eine Substitution auf verschiedene Arten in Transpositionsfolgen zerlegt wird, die Anzahl der Transpositionen stets eine gerade oder stets eine ungerade ist, je nachdem nämlich die Substitution das Zeichen von $\sqrt{D}$ ungeändert lässt oder nicht. Demnach kann man widerspruchsfrei gerade oder ungerade Substitutionen als solche definiren, welche in eine gerade oder in eine ungerade Anzahl von Transpositionen zerlegbar sind. Die Einheitssubstitution gehört zu den geraden Substitutionen; denn sie lässt ψ ungeändert. Dasselbe erkennt man aus dem Beispiele des vorigen Paragraphen.

Sind unter den $n!$ überhaupt vorhandenen Substitutionen der n Elemente z_α,

$g_1, g_2, \cdots g_\mu$ die geraden Substitutionen
$u_1, u_2, \cdots u_\nu$ „ ungeraden „ $\qquad (\mu + \nu = n!)$

und bedeutet t eine beliebige Transposition, so sind alle $g_\alpha t$ von einander verschiedene ungerade Substitutionen, und daher ist $\nu \geqq \mu$. Ebenso sind alle $u_\alpha t$ von einander verschiedene gerade Substitutionen, und daher ist $\mu \geqq \nu$. Folglich ist $\mu = \nu = \frac{1}{2} n!$. Es giebt ebenso viele gerade wie ungerade Substitutionen, nämlich von jeder Art $\frac{1}{2} n!$. Da g_α und g_β die Function nicht ändern, so thut es auch $g_\alpha \cdot g_\beta$ nicht, d. h. dieses Product gehört wieder unter die g. Nach § 518, Schluss besteht daher die Gruppeneigenschaft auch für die g; demnach können wir sagen: Alle geraden Substitutionen bilden eine Gruppe der Ordnung $\frac{1}{2} n!$; wir werden sie als alternirende Gruppe bezeichnen.

§ 521. Es sei nun χ irgend eine ganze, zweiwerthige Function der Variablen z, d. h. eine solche, die unter dem Einflusse aller $n!$ Substitutionen ihrer Elemente z zwei und nur zwei ihrer Form nach verschiedene Werthe annimmt; χ_1 und χ_2 seien diese beiden Werthe.

Aendert eine Substitution s den Werth χ_1 nicht, dann kann sie auch χ_2 nicht in χ_1 umändern, weil sonst s^{-1} gleichzeitig χ_1 änderte und doch nicht änderte. Ebenso wird eine Substitution, welche χ_1 in χ_2 umwandelt, umgekehrt χ_2 in χ_1 überführen. Deshalb ist $(\chi_1 - \chi_2)$ gleichfalls eine zweiwerthige Function und zwar eine alternirende, da ihr zweiter Werth $(\chi_2 - \chi_1)$ wird. Ferner ist $(\chi_1 + \chi_2)$ eine symmetrische Function. Wir können demnach

$$(5) \qquad \begin{aligned} \chi_1 + \chi_2 &= 2 S_0 \quad, \quad & \chi_1 - \chi_2 &= 2 S_1 \sqrt{D}; \\ \chi_1 &= S_0 + S_1 \sqrt{D}, & \chi_2 &= S_0 - S_1 \sqrt{D} \end{aligned}$$

setzen und erkennen: Jede zweiwerthige, ganze Function ist von der Form

$$\chi = S_0 \pm S_1 \sqrt{D},$$

in welcher S_0, S_1 beliebige ganze, symmetrische Functionen bedeuten. Also ist χ Wurzel der quadratischen Gleichung

$$\chi^2 - 2 S_0 \cdot \chi + (S_0^2 - S_1^2 D) = 0.$$

χ bleibt bei allen geraden Substitutionen und nur bei diesen ungeändert. Jede zweiwerthige Function ist durch jede andere als ganze, lineare Function darstellbar, deren Coefficienten gebrochene, symmetrische Functionen sind. Wir rechnen alle zweiwerthigen Functionen zu einer Gattung, der „alternirenden Gattung“.

§ 522. Bevor wir zur Behandlung anderer Functionengattungen übergehen, wird es gut sein, statt der schwerfälligen Schreibweise für Substitutionen, die wir durch (1) in § 518 eingeführt haben, eine expeditere zu erläutern und zu benutzen. Wenn durch (1) das Element z_a in z_b, dieses in z_c, dieses in z_d, $\cdots$ übergeführt wird, so muss man einmal auf ein Element z_g stossen, welches wieder in z_a übergeht. Denjenigen Theil der Substitution, welcher die angegebenen Umwandlungen umfasst, schreiben wir $(z_a z_b z_c \cdots z_g)$ und nennen dies einen Cyklus; denkt man sich die Elemente desselben in gleichen Abständen auf einem Kreise angeordnet, so kann man die Wirkung eines Cyklus als Drehung des Kreises um sein Centrum auffassen. Hat der Cyklus m Elemente, so ist die Grösse der Drehung $\frac{2\pi}{m}$. Wir nennen diese Anzahl m die Ordnung des Cyklus. Offenbar ist

$$(z_a z_b z_c \cdots z_g) = (z_b z_c \cdots z_g z_a) = (z_c \cdots z_g z_a z_b) = \cdots.$$

Die Transpositionen sind Cyklen zweiter Ordnung.

Giebt es in der Substitution noch andere Elemente ausser den in dem hergestellten Cyklus vorkommenden, so geben diese Veranlassung zu einem weiteren Cyklus u. s. f., und so lässt sich (1) in eine Anzahl von Cyklen zerlegen, von denen keiner mit einem anderen ein Element gemeinsam hat. Wenn in (1) ein $i_\alpha = \alpha$ ist, so erscheint in der cyklischen Darstellung ein Cyklus der Ordnung 1; falls anderweitig feststeht, welche Elemente der Substitution unterworfen sind, kann man alle solche Cyklen von der Ordnung 1 unterdrücken. Jede Substitution, die abgesehen von Cyklen der Ordnung 1 nur aus einem einzigen Cyklus besteht, heisst eine cyklische Substitution.

Wir wollen diese neue Schreibweise beim Beweise einiger Eigenschaften der alternirenden Gruppe verwenden (§ 519). Einen Cyklus k^{ter} Ordnung kann man in $(k-1)$ Transpositionen zerlegen

$$(z_1 z_2 \cdots z_k) = (z_1 z_2)(z_1 z_3) \cdots (z_1 z_k);$$

daher gehört eine, aus einem einzigen Cykel bestehende Substitution der alternirenden Gruppe an oder nicht, je nachdem die Ordnung des Cykels ungerade oder gerade ist. Dies ergiebt: Eine Substitution gehört der alternirenden Gruppe an oder nicht, je nachdem sie eine gerade oder eine ungerade Anzahl von Cyklen gerader Ordnung enthält.

Der oben (§ 519) abgeleitete Satz, dass jede Function, die bei allen Transpositionen ungeändert bleibt, eine symmetrische Function sei, kann auch so ausgesprochen werden: Jede Gruppe, welche alle Transpositionen enthält, ist die symmetrische Gruppe.

Ja, es reicht dafür schon aus, dass die Gruppe die $(n-1)$ Transpositionen

$$(z_1 z_2),\ (z_1 z_3),\ (z_1 z_4),\ \cdots\ (z_1 z_n)$$

enthält, da jedes

$$(z_h z_k) = (z_1 z_h)(z_1 z_k)(z_1 z_h)$$

ist.

Als Analogon hierzu stellen wir das Theorem auf: **Jede Gruppe, welche alle cyklischen Substitutionen dritter Ordnung enthält, ist entweder alternirend oder symmetrisch.** Denn jede Substitution der alternirenden Gruppe kann in eine gerade Anzahl von Transpositionen zerlegt werden; fasst man die beiden ersten dieser Transpositionen zusammen, dann die beiden folgenden u. s. f., so erhält man Paare von einer der drei Bildungsgestalten

$$(z_a z_b)(z_a z_b),\quad (z_a z_b)(z_a z_c),\quad (z_a z_b)(z_c z_d).$$

Die erste Form ist der Einheit äquivalent und kann daher unterdrückt werden; die zweite ist einem Cykel dritter Ordnung $(z_a z_b z_c)$ äquivalent; die dritte ist gleich $(z_a z_b)(z_a z_c)\cdot(z_c z_a)(z_c z_d)$ und also zwei Cyklen dritter Ordnung äquivalent. Demnach ist die Substitution durch Cyklen dritter Ordnung darstellbar. Damit ist der Beweis des aufgestellten Satzes geliefert.

Ebenso kann man zeigen: **Jede Gruppe, welche alle cyklischen Substitutionen fünfter Ordnung enthält, ist alternirend oder symmetrisch.** Es folgt dies einfach aus der Darstellung

$$(z_1 z_2 z_3) = (z_1 z_4 z_3 z_5 z_2)(z_1 z_3 z_4 z_2 z_5).$$

Offenbar kann man in der Reihe dieser Sätze weiter gehen. —

Ferner zeigt sich: **Jede Gruppe, welche alle cyklischen Substitutionen vierter Ordnung oder alle diejenigen sechster Ordnung u. s. w. enthält, ist symmetrisch.** Denn man hat der Reihe nach

$$\begin{aligned}(z_1 z_2) &= (z_1 z_2 z_3 z_4)(z_1 z_3 z_2 z_4)(z_1 z_3 z_4 z_2)\\ &= (z_1 z_2 z_3 z_4 z_5 z_6)(z_1 z_3 z_2 z_4 z_5 z_6)(z_1 z_5 z_3 z_6 z_4 z_2)\\ &\quad \cdots\cdots\cdots\cdots\end{aligned}$$

und daher enthält diese Gruppe auch sämmtliche Transpositionen in sich. —

Endlich erwähnen wir noch, dass die **Potenzbildung** sich bei Cyklen rechnerisch ausserordentlich einfach vollzieht. So ist für $s = (z_1 z_2 z_3 z_4 z_5 z_6)$ sofort zu sehen, dass man hat

$$\begin{aligned}s^2 &= (z_1 z_3 z_5)(z_2 z_4 z_6), & s^3 &= (z_1 z_4)(z_2 z_5)(z_3 z_6), & \\ s^4 &= (z_1 z_5 z_3)(z_2 z_6 z_4), & s^5 &= (z_1 z_6 z_5 z_4 z_3 z_2), & s^6 = 1.\end{aligned}$$

§ 523. Wir gehen jetzt zu einer anderen für uns wichtigen Art von Functionen über, zu den cyklischen. Wir denken uns die Variablen in eine beliebige aber feste Reihenfolge gebracht, etwa in die natürliche $z_1, z_2, \cdots z_{n-1}, z_n$, und fragen nach den ganzen Functionen der z_α, welche ungeändert bleiben, wenn man auf sie die cyklische Substitution

$$(6)\qquad s = (z_1 z_2 \cdots z_{n-1} z_n)$$

anwendet. Natürlich bleibt eine solche Function auch für die Potenzen von s, nämlich für sämmtliche

$$(6^a)\qquad s^k = (z_1 z_{k+1} \cdots z_\alpha z_{\alpha+k} \cdots) \qquad (k = 1, 2, \cdots n)$$

ungeändert, die nicht alle cyklisch zu sein brauchen.

Bei der getroffenen Anordnung der z lässt sich eine noch einfachere Bezeichnung von s an die Stelle von (6) und (6ª) setzen, indem man

$$(6^b)\qquad s = |z_\alpha \quad z_{\alpha+1}|, \quad s^k = |z_\alpha \quad z_{\alpha+k}| \qquad (\alpha = 1, 2, \cdots n)$$

schreibt. Hierbei müssen alle Indices, welche grösser als n sind, durch ihre kleinsten, positiven Reste modulo n ersetzt werden. — Die Potenz s^k ist dann und nur dann gleichfalls cyklisch, wenn die Reihe

$$0, k, 2k, \cdots (n-1)k \pmod{n}$$

alle Indices $1, 2, \cdots (n-1), n$ umfasst, d. h. wenn k zu n theilerfremd ist. — Den Indices $1, 2, \cdots n$ der Variablen z kann man $n!$ verschiedene Anordnungen ertheilen. Ist $i_1, i_2, \cdots i_n$ eine derselben, so liefert $(z_{i_1} z_{i_2} \cdots z_{i_n}) = |z_{i_\alpha} \quad z_{i_{\alpha+1}}|$ eine cyklische Substitution; es giebt also für n Elemente $n!$ cyklische Substitutionen. Da aber bei einer jeden das Anfangsglied beliebig unter ihren Elementen gewählt werden kann, so haben je n denselben Effect, und es giebt nur $(n-1)!$ von einander verschiedene. Für 4 Elemente also bestehen z. B. die folgenden 6 cyklischen Substitutionen:

$$(z_1 z_2 z_3 z_4), \quad (z_1 z_2 z_4 z_3), \quad (z_1 z_3 z_2 z_4),$$
$$(z_1 z_3 z_4 z_2), \quad (z_1 z_4 z_2 z_3), \quad (z_1 z_4 z_3 z_2).$$

Die n Potenzen s^k (6ª) bilden eine Gruppe der Ordnung n; sie heisst die cyklische Gruppe oder genauer: die zu der getroffenen Elementenanordnung gehörige cyklische Gruppe. Eine ganze Function, welche ihre Form unter dem Einflusse der Substitutionen der cyklischen Gruppe nicht ändert, heisst eine für diese Elementenanordnung cyklische Function. Es ist leicht, derartige Functionen zu bilden.

Bedeuten α und β von einander verschiedene positive Zahlen, so wird eine solche z. B.

$$(7) \qquad \varphi = z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + \cdots + z_{n-1}^\alpha z_n^\beta + z_n^\alpha z_1^\beta$$

Dass (7) durch s und seine Potenzen nicht geändert wird, ist augenscheinlich. Umgekehrt ist jede Substitution σ, welche die Form von (7) nicht ändert, eine Potenz von s. Denn führt sie z_1 in z_{k+1} und z_2 in z_l über, so wird $z_1^\alpha z_2^\beta$ in $z_{k+1}^\alpha z_l^\beta$ umgewandelt. Da hierbei die Form von φ gewahrt bleiben soll, so muss dieses umgewandelte Glied mit $z_{k+1}^\alpha z_{k+2}^\beta$ übereinstimmen, d. h. z_2 geht durch σ in z_{k+2} über; daraus folgt ebenso, dass z_3 in z_{k+3} verwandelt wird, u. s. f.; die Substitution σ ist demnach mit $s^k = | z_\alpha \;\; z_{\alpha+k} |$ identisch. —

Eine andere Art von Functionen, welche gleichfalls unseren Forderungen entspricht, wird für jede von ± 1 verschiedene Constante c die Function werden

$$(8) \qquad \psi = (z_1 + cz_2)(z_2 + cz_3) \cdots (z_{n-1} + cz_n)(z_n + cz_1).$$

Auch diese bleibt für s und seine Potenzen ungeändert. Bleibt umgekehrt ψ für eine Substitution σ ungeändert, so braucht zwar nicht jeder Factor der ursprünglichen Form wieder in einen solchen umgewandelt zu werden, aber dies muss wenigstens bis auf einen constanten Factor geschehen, und das Product aller constanten Factoren bei sämmtlichen Klammern muss gleich 1 werden. Verwandelt nun σ das Element z_1 in z_{k+1} und z_2 in z_l, so geht $(z_1 + cz_2)$ in $(z_{k+1} + cz_l)$ über. Dies wird also entweder gleich $(z_{k+1} + cz_{k+2})$ oder gleich $(z_{k+1} + cz_k)$, abgesehen von constanten Factoren, sein müssen. Der erste Fall führt, gerade wie oben bei (7), sofort darauf, dass σ eine Potenz von s ist. Der zweite fordert, dass z_2 in z_k übergeht, und dass $c\left(z_k + \frac{1}{c} z_{k+1}\right)$ bis auf den Factor c mit $(z_k + cz_{k+1})$ identisch wird. Hierzu müsste $c = \pm 1$ sein, was oben ausgeschlossen wurde. Folglich kann die zweite Annahme sich nicht verwirklichen. —

Eine dritte Art hierher gehöriger Functionen wird durch die **Lagrange**'sche Resolvente geliefert. In der That bleibt der Ausdruck

$$(9) \qquad \varpi^n = (z_1 + \omega z_2 + \omega^2 z_3 + \cdots + \omega^{n-1} z_n)^n,$$

in dem ω eine primitive n^{te} Einheitswurzel bedeutet, für s und seine Potenzen ungeändert; und wenn umgekehrt σ eine Substitution bezeichnet, welche ϖ^n nicht ändert, so kann sie die Klammergrösse ϖ selbst höchstens mit einer n^{ten} Einheitswurzel ω^λ multipliciren, wenn sie überhaupt eine Aenderung hervorruft. Setzen wir also, um diese Möglichkeit zu untersuchen,

$$\sigma = \begin{pmatrix} z_1 & z_2 & \cdots & z_n \\ z_{i_1} & z_{i_2} & \cdots & z_{i_n} \end{pmatrix},$$

so müsste die Gleichung

$$z_{i_1} + \omega z_{i_2} + \omega^2 z_{i_3} + \cdots + \omega^{n-1} z_{i_n}$$
$$= \omega^\lambda z_1 + \omega^{\lambda+1} z_2 + \omega^{\lambda+2} z_3 + \cdots + \omega^{\lambda-1} z_n$$

gelten. Da alle Potenzen von ω links wie rechts jedesmal untereinander verschieden sind, so folgt hieraus $z_{i_1} = z_{n+1-\lambda}$, $z_{i_2} = z_{n+2-\lambda}, \cdots$, und es ist $\sigma = s^{n-\lambda}$.

§ 524. Wir können den Begriff der cyklischen Substitutionen und der cyklischen Gruppen auf folgende Art erweitern*). Es mögen $N = n_1 \cdot n_2 \cdots n_\nu$ Grössen

(10) $$z_{h_1, h_2, \cdots h_\nu} \qquad (h_\alpha = 1, 2, 3, \cdots n_\alpha;\ \alpha = 1, 2, \cdots \nu)$$

gegeben sein. Dann heisst eine Substitution s in weiterem Sinne cyklisch, wenn sie hinsichtlich jedes der ν Indices h_α cyklisch im oben festgesetzten Sinne ist. Der Bezeichnung (6^b) entsprechend können wir hier eine Erweiterung einführen, indem wir unter

(11) $$\left| z_{h_1, h_2, \cdots h_\nu} \quad z_{h_1+\alpha_1, h_2+\alpha_2, \cdots h_\nu+\alpha_\nu} \right| = s_{\alpha_1, \alpha_2, \cdots \alpha_\nu}$$

diejenige Substitution verstehen, welche den ersten Index jedes z um die Grösse α_1, den zweiten Index eines jeden z um α_2, u. s. w. vermehrt; dabei ist jedesmal, wenn der erste Index n_1 übertreffen würde, sein kleinster positiver Rest mod. n_1 zu setzen, und ähnlich bei den weiteren Indices**). Man erkennt sofort, dass $s_{\alpha_1, \alpha_2, \ldots}$ sich aus den ν Substitutionen, bei denen nur ein Index um 1 vermehrt wird,

(12) $$s_\mu = \left| z_{h_1, \cdots h_\mu, \cdots h_\nu} \quad z_{h_1, \cdots h_\mu+1, \cdots h_\nu} \right| \qquad (\mu = 1, 2, \cdots \nu)$$

zusammensetzen lässt. Denn es wird ja, indem man die Potenzen und Potenzproducte bildet

(13) $$s_1^{\alpha_1} = \left| z_{h_1, h_2, \cdots h_\nu} \quad z_{h_1+\alpha_1, h_2, \cdots h_\nu} \right|, \quad s_2^{\alpha_2} = \left| z_{h_1, h_2, \cdots h_\nu} \quad z_{h_1, h_2+\alpha_2, \cdots h_\nu} \right|;$$
$$s_1^{\alpha_1} s_2^{\alpha_2} = \left| z_{h_1, h_2, h_3, \cdots h_\nu} \quad z_{h_1+\alpha_1, h_2+\alpha_2, h_3, \cdots h_\nu} \right|; \quad \text{u. s. f.}$$

Man bemerkt ferner leicht, dass es eine und auch nur eine unter den Substitutionen (11) giebt, welche ein beliebiges $z_{k_1, k_2, \ldots}$ in ein beliebiges $z_{l_1, l_2, \ldots}$ umwandelt, nämlich $s_1^{l_1-k_1} s_2^{l_2-k_2} \cdots$. Insbesondere giebt es also nur eine Substitution, nämlich die Einheit, welche ein

*) Vgl. Kronecker, Berl. Ber. 1877; Nachtrag zum Decemberheft, S. 846 ff.

**) Cauchy nennt (Exercices III, p. 232) die Substitution (11) eine „arithmetische" Substitution.

beliebiges Element nicht ändert; d. h. ausser der Einheit setzt jede Substitution (11) alle Elemente z um.

Lässt man negative Indices zu, so folgt die Relation

$$s_{\alpha_1, \alpha_2, \cdots} \cdot s_{-\alpha_1, -\alpha_2, \cdots} = 1.$$

Wir können daher den zweiten Factor mit $s^{-1}_{\alpha_1, \alpha_2, \cdots}$ bezeichnen.

Das Product zweier Substitutionen (11) besitzt wieder die Form (11); es gilt das commutative und das associative Gesetz. Alle Substitutionen (11) bilden eine Abel'sche Gruppe von der Ordnung $N = n_1 \cdot n_2 \cdots n_\nu$. Dies ist die erweiterte cyklische Gruppe.

Eine rationale Function der N Grössen z soll eine cyklische Function in weiterem Sinne heissen, wenn sie unter der Einwirkung aller Substitutionen (11) ungeändert bleibt, sich dagegen bei jeder anderen Substitution ändert. Erfüllt eine rationale Function die erste Bedingung, bleibt sie aber noch bei anderen Substitutionen ausser (11) ungeändert, dann sagen wir, sie steht unter den cyklischen Functionen.

Theoretisch am einfachsten stellen wir cyklische Functionen in weiterem Sinne auf folgende Art her. Wir bilden ein Glied

$$Z_1 = \prod_{(h)} z_{h_1 \cdots h_\nu}^{\alpha_{h_1 \cdots h_\nu}} \qquad (h_\alpha = 1, 2, \cdots n_\alpha;\ \alpha = 1, 2, \cdots \nu),$$

in welchem die α beliebige ganze, positive, von einander verschiedene Zahlen bedeuten, wenden auf Z_1 alle Substitutionen (11) an derart, dass bei festen Exponenten die unteren Indices vertauscht werden, und erhalten dadurch die Glieder $Z_1, Z_2, Z_3, \cdots Z_N$. Dann liefert die Summe

$$\varphi = Z_1 + Z_2 + \cdots + Z_k + \cdots + Z_N$$

eine Function von den verlangten Eigenschaften.

Dass φ für alle Substitutionen (11) ihre Form beibehält, folgt aus ihrer Herstellungsweise.

Nun möge umgekehrt eine Substitution σ von noch unbekannter Gestalt die Form von φ nicht ändern; durch sie möge $z_{11\cdots}$ in $z_{k_1+1, k_2+1, \cdots}$ übergehen, und also $z_{11\cdots}^{\alpha_{11\cdots}}$ in $z_{k_1+1, k_2+1, \cdots}^{\alpha_{11\cdots}}$. Unter den Z kommt nur ein einziges Glied vor, welches $z_{k_1+1, k_2+1, \cdots}^{\alpha_{11\cdots}}$ enthält, etwa Z_k. Dann ist es nothwendig, dass σ das Glied Z_1 in Z_k verwandelt. Durch diesen Uebergang ist aber jedes z_α in ein bestimmtes z_β übergeführt, d. h. σ setzt alle z_α in dieselben z_β um, wie jene Substitution (11) die Z_1 in Z_k transformirte; d. h. σ ist mit dieser Substitution aus (11) identisch.

Einfachere Functionen als jenes φ kann man auf mancherlei Weise erhalten, z. B. wenn man das eben benutzte Z_1 durch

$$Z_1' = z_{111\ldots}^{\alpha_0} z_{211\ldots}^{\alpha_1} z_{121\ldots}^{\alpha_2} z_{112\ldots}^{\alpha_3} \cdots$$

ersetzt; doch gestaltet sich der Beweis hier etwas umständlicher, so dass wir auf diese Dinge nicht eingehen wollen.

Nur die hierher gehörige Verallgemeinerung der Lagrange'schen Resolvente wollen wir noch besprechen (vgl. § 321, Bd. I).

Wir verstehen unter $\omega_1, \omega_2, \cdots$ primitive $n_1^{\text{te}}, n_2^{\text{te}}, \cdots$ Einheitswurzeln und bilden mit diesen die Function

$$(14)\quad \varpi^{n_1 n_2 \cdots} = \Big[\sum_{(h)} \omega_1^{h_1-1} \omega_2^{h_2-1} \cdots z_{h_1, h_2, \cdots}\Big]^{n_1 n_2 \cdots} \qquad (h_\alpha = 1, 2, \cdots n_\alpha);$$

dann folgt zunächst, dass (14) für jedes s aus (11) ungeändert bleibt. Denn wenn man ein s_μ aus (12) anwendet, dann kann man die Schlüsse des vorigen Paragraphen wiederholen. Die Verwendung von s_1 liefert z. B.

$$\sum_{h_2, h_3, \cdots} \omega_2^{h_2-1} \cdots \sum_{h_1} \omega_1^{h_1-1} z_{h_1+1, h_2, \cdots} = \omega_1^{-1} \sum_{h_2, h_3, \cdots} \omega_2^{h_2-1} \cdots \sum_{h_1} \omega_1^{h_1-1} z_{h_1, h_2, \cdots}$$
$$= \omega_1^{-1} \varpi,$$

so dass (14) wegen der Bedeutung von ω_1 ungeändert bleibt.

Wenn umgekehrt eine Substitution σ von noch unbekannter Gestalt (14) nicht ändert, dann kann sie ϖ selbst nur mit einer $(n_1 \cdot n_2, \cdots)^{\text{ten}}$ Einheitswurzel multipliciren, etwa mit $\omega_1^{-\alpha_1} \omega_2^{-\alpha_2} \cdots$; in diesem Falle muss die Klammergrösse aus (14) in die Summe

$$\sum_{(h)} \omega_1^{h_1-\alpha_1-1} \omega_2^{h_2-\alpha_2-1} \cdots z_{h_1, h_2, \cdots} = \sum_{(h)} \omega_1^{h_1-1} \omega_2^{h_2-1} \cdots z_{h_1+\alpha_1, h_2+\alpha_2, \cdots}$$

übergehen, d. h. es ist, wie behauptet wurde, die vermittelnde Substitution nämlich

$$\sigma = \left| z_{h_1, h_2, \cdots} \quad z_{h_1+\alpha_1, h_2+\alpha_2, \cdots} \right|$$

eine der verallgemeinerten cyklischen Substitutionen (11). —

Einleuchtend ist es auch, wovon wir bald Gebrauch machen werden, dass die Function

$$(14^{\text{a}})\quad \varpi_{k_1, k_2, \cdots} = \sum_{(h)} \omega_1^{k_1(h_1-1)} \omega_2^{k_2(h_2-1)} \cdots z_{h_1, h_2, \cdots} \qquad (h_\alpha = 1, 2, \cdots n_\alpha)$$

unter dem Einflusse jedes (11) nur eine Einheitswurzel als Factor erhält, was $k_1, k_2, \cdots$ auch immer für ganze Zahlen bedeuten mögen. Dieser Factor ist bei der Verwendung von $s_1^{\alpha_1} s_2^{\alpha_2} \cdots$ gleich $\omega_1^{-\alpha_1} \omega_2^{-\alpha_2} \cdots$ und also von $k_1, k_2, \cdots$ unabhängig.

Wir haben gesehen, dass die Anzahl der Substitutionen (11) gleich $N = n_1 \cdot n_2 \cdots n_\nu$ ist, also gleich der Anzahl der Elemente z selbst. Nach § 508, E) schliesst man daraus, worauf wir in der nächsten Vorlesung noch ausführlich eingehen werden, dass jede Function φ, welche cyklisch in weiterem Sinne ist, aber nicht unter den cyklischen Functionen steht, welche also für alle (11) und nur für diese Substitutionen ungeändert bleibt, unter dem Einflusse sämmtlicher $N!$ Substitutionen der N Elemente genau $M = (N-1)!$ Werthe $\varphi_1, \varphi_2, \cdots$ besitzt. Diese sind Wurzeln einer Gleichung

$$(15) \qquad \begin{aligned} G(\varphi) &= \varphi^M - A_1 \varphi^{M-1} + A_2 \varphi^{M-2} - \cdots \pm A_M \\ &= (\varphi - \varphi_1)(\varphi - \varphi_2) \cdots = 0, \end{aligned}$$

deren Coefficienten symmetrische Functionen der sämmtlichen Elemente z werden.

Jede Function χ der N Grössen z, welche in der gegebenen Anordnung erweitert-cyklisch ist, oder auch unter den cyklischen Functionen der Form (11) steht, ist nun rational durch φ, d. h. durch jede beliebige zu (11) gehörige cyklische Function darstellbar, sobald man die symmetrischen Functionen der sämmtlichen Elemente z dem Rationalitätsbereiche zugeordnet denkt. Dies folgt genau durch dieselben Schlüsse, wie sie z. B. in § 490 verwendet sind, nämlich durch die Betrachtung des Productes

$$G(\varphi)\left[\frac{\chi_1}{\varphi - \varphi_1} + \frac{\chi_2}{\varphi - \varphi_2} + \cdots\right] = H(\varphi),$$

in welchem φ eine Variable bedeutet. Da wir auch diesen Satz allgemein in einer der nächsten Vorlesungen besprechen, so reicht es für jetzt aus, die folgenden Punkte hervorzuheben. Die Klammer auf der linken Seite ist, ebenso wie der Factor $G(\varphi)$, eine symmetrische Function sämmtlicher z; die gesammte linke Seite wird eine ganze Function, wenn χ eine solche ist; die Werthe $\varphi_1, \varphi_2, \cdots$ sind alle untereinander verschieden, während die χ zum Theil einander gleich werden können. Setzt man also $\varphi = \varphi_1$, so erhält man aus der letzten Gleichung

$$\chi_1 = \frac{H(\varphi_1)}{G'(\varphi_1)}.$$

§ 525. Versteht man unter $f_1', f_1'', \cdots f_1^{(\alpha)}, \cdots$ eine Reihe von $N = n_1 \cdot n_2 \cdots n_\nu$ rationalen Functionen der N Variablen z, ordnet sie in einer Zeile an und wendet nun auf diese Functionenreihe alle N Substitutionen s von (11) an, so entstehen N Zeilen

$$(16) \qquad \begin{array}{l} f_1', \ f_1'', \ \cdots \ f_1^{(\alpha)}, \ \cdots, \\ f_2', \ f_2'', \ \cdots \ f_2^{(\alpha)}, \ \cdots, \\ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \end{array}$$

und das so erhaltene Schema hat die Eigenthümlichkeit, dass bei der Verwendung jedes unserer s aus (11) nur die Zeilen von (16) in einander übergehen. Die Art dieses Ueberganges hängt dabei lediglich von den s, nicht aber von den Functionen f ab. Macht man nun aus der Matrix (16) unter Beibehaltung der Anordnung der Elemente eine Determinante

$$\Delta = \left| f_\varkappa^{(\lambda)} \right| \qquad (\varkappa, \lambda = 1, 2, \cdots N),$$

so wird diese unter dem Einflusse unserer erweiterten cyklischen Substitutionen $s_{\alpha\beta\ldots}$ von (11) entweder ungeändert bleiben oder lediglich ihr Vorzeichen ändern. Ist also Δ_1 eine aus einem anderen Functionensysteme ähnlich gebildete Determinante, dann bleibt sowohl $\Delta \cdot \Delta_1$ wie $\Delta : \Delta_1$ für die erweiterte cyklische Gruppe ungeändert, da ja wegen der Anordnung der Zeilen beide Determinanten entweder gleichzeitig sich ändern oder gleichzeitig unverändert bleiben. Infolge des allgemeinen Theorems aus dem vorigen Paragraphen werden daher $\Delta \cdot \Delta_1$ und $\Delta : \Delta_1$ rational durch irgend welche cyklische Function darstellbar sein.

§ 526. Nun möge f_1 eine beliebige rationale Function der N Grössen z bedeuten. Wir wollen versuchen, sie andererseits auch als eine lineare Function der $z_{h,k,\ldots}$ darzustellen, deren Coefficienten dann natürlich nicht constant sein können, die wir aber, wenn das möglich ist, so bestimmen wollen, dass sie cyklisch sind oder unter den cyklischen Functionen stehen. Wir fordern also Coefficienten A, durch welche die Gleichung befriedigt wird:

$$(17) \qquad f_1 = \sum A_{h_1, h_2, \ldots} \; z_{h_1, h_2, \ldots}, \qquad (h_\alpha = 1, 2, \cdots n_\alpha);$$

derart dass sich hierbei die $A_{h_1, h_2, \ldots}$ nicht für die cyklischen Substitutionen (11) ändern. Wendet man die (11) nun sämmtlich auf (17) an, so entstehen daraus N in ebenso vielen A lineare Gleichungen, durch deren Auflösung die Bestimmung dieser unbekannten Coefficienten geliefert wird. Ein jeder wird dabei die Form eines Quotienten $\Delta : \Delta_1$ annehmen, wie wir ihn im vorigen Paragraphen behandelt haben und also thatsächlich cyklisch werden oder unter den cyklischen Functionen stehen. Es handelt sich nur noch darum festzustellen, dass die Determinante, welche in den Nenner tritt, nämlich

$$\Delta_1 = \left| z_{h_1 + k_1, h_2 + k_2, \cdots} \right|$$

bei allgemeinen z von Null verschieden ist. Dies beweisen wir so: Wir betrachten die vier Schnittelemente der ersten und der α^{ten} Spalte mit der ersten und der β^{ten} Zeile, nämlich

$$z_{1,1,1,\cdots}, \qquad z_{h_1,h_2,h_3,\cdots},$$
$$z_{k_1,k_2,k_3,\cdots}, \qquad z_{h_1+k_1-1,\,h_2+k_2-2,\cdots}.$$

Jede der Zeilen von Δ_1 multipliciren wir mit dem folgenden Factor, in welchem $\tau_1, \tau_2, \tau_3, \cdots$ feste Zahlen sein sollen,

$$\omega_1^{\tau_1(k_1-1)}\omega_2^{\tau_2(k_2-1)}\omega_3^{\tau_3(k_3-1)}\cdots,$$

dessen $k_1, k_2, \cdots$ dem Anfangsgliede der Zeile entsprechen; ebenso multipliciren wir jede der Spalten von Δ_1 mit einem Factor

$$\omega_1^{\tau_1(h_1-1)}\omega_2^{\tau_2(h_2-1)}\omega_3^{\tau_3(h_3-1)}\cdots,$$

dessen $h_1, h_2, \cdots$ dem Anfangsgliede der Spalte entsprechen. Dadurch wird das Schnittglied der Spalte und der Zeile mit dem Factor

$$\omega_1^{\tau_1(k_1+h_1-2)}\omega_2^{\tau_2(k_2+h_2-2)}\cdots$$

multiplicirt; das entspricht aber genau dem Gliede selbst. Es ist somit

$$\Omega\Delta_1 = \left|\omega_1^{\tau_1(h_1+k_1-1)}\omega_2^{\tau_2(h_2+k_2-1)}\cdots z_{h_1+k_1,\,h_2+k_2,\cdots}\right|,$$

wobei Ω eine N^{te} Einheitswurzel bedeutet, und jedes $\tau_\alpha = 1, 2, \cdots n_\alpha$ genommen werden kann. Addirt man hier die Elemente der zweiten, dritten, $\cdots$ Spalte zu den entsprechenden der ersten, so enthält diese nur gleiche Elemente, nämlich $\varpi_{\tau_1,\tau_2,\cdots}$ (vgl. 14[a]). Es tritt also $\varpi_{\tau_1,\tau_2,\cdots}$ als Factor von Δ_1 heraus; ferner erhält man, da $\tau_1, \tau_2, \cdots$ an Werthecombinationen N_1 aufweisen, und da jedes solche ϖ herausgezogen werden kann,

$$\Delta_1 = \text{const.}\prod_{(\tau)}\varpi_{\tau_1,\tau_2,\cdots} \qquad (\tau_\alpha = 1, 2, \cdots n_\alpha).$$

Dass die Constante nicht verschwindet, folgt, sobald man eins der z gleich 1 und die übrigen gleich 0 setzt. Die ϖ sind lineare Functionen, welche bei allgemeinen z nicht verschwinden. Der auftretende Nenner ist demnach von Null verschieden, und wir können sagen*): Jede rationale Function der Grössen $z_{h_1,h_2,\cdots h_\nu}$ lässt sich als lineare homogene Function derselben Grössen so darstellen, dass ihre Coefficienten ungeändert bleiben für die cyklischen Substitutionen

$$(11) \qquad \left|z_{h_1,h_2,\cdots h_\nu} \quad z_{h_1+\alpha_1,\,h_2+\alpha_2,\cdots h_\nu+\alpha_\nu}\right| = s_{\alpha_1,\alpha_2,\cdots\alpha_\nu}.$$

§ 527. Die erlangten Resultate können wir jetzt dazu verwenden, um die Abel'schen Gleichungen von einer neuen Seite her zu beleuchten.

---

*) Kronecker, Berl. Ber. 1877; Nachtr. z. Decemberheft, p. 847.

Es sei z eine Variable; ferner seien $N = n_1 \cdot n_2 \cdots n_\nu$ feste Grössen $z_{h_1, h_2, \cdots h_\nu}$ gegeben; jedes h_α ist mod. n_α auf seinen kleinsten, positiven Rest zu reduciren. Wir setzen das Product an

$$\mathfrak{F}(z) = \prod_{(h)} [z - z_{h_1, h_2, \cdots h_\nu}] \qquad (h_\alpha = 1, 2, \cdots n_\alpha).$$

Die Coefficienten dieser Gleichung sollen dem Rationalitätsbereiche angehören; eine genauere Bestimmung für sie wird bald erfolgen.

Ferner nehmen wir ein

$$\Theta_\alpha(z) = \sum_{(h)} z_{h_1, \cdots h_\alpha + 1, \cdots h_\nu} \frac{\mathfrak{F}(z)}{z - z_{h_1, h_2, \cdots h_\nu}} \frac{1}{\mathfrak{F}'(z_{h_1, h_2, \cdots h_\nu})},$$

derart dass die Summation über alle N Combinationen der Werthe der h sich erstreckt. Dadurch wird $\Theta_\alpha(z)$ zu einer ganzen Function von z, welche entweder direct cyklisch ist, oder doch unter den cyklischen Functionen steht. Denn vermehrt man in dem hingeschriebenen Term irgend einen der Indices h um eine beliebige ganze Zahl, so kommt wieder ein Glied der hingeschriebenen Summe heraus.

Die Bedeutung der $\Theta_\alpha(z)$ für die Beziehung der Wurzeln von $\mathfrak{F} = 0$ untereinander zeigt sich leicht. Vergleicht man die obige Darstellung mit der Lagrange'schen Interpolationsformel, so folgt, was auch die unmittelbare Anschauung zeigt, sofort

$$\Theta_\alpha(z_{h_1, h_2, \cdots h_\nu}) = z_{h_1, \cdots h_\alpha + 1, \cdots h_\nu}.$$

Ferner erhält man hieraus, wenn die λ-mal iterirte Function Θ mit $\Theta^{(\lambda)}$ bezeichnet wird, die Relationen

$$\Theta_\alpha^{(\lambda)} \Theta_\beta^{(\mu)} (z_{h_1, h_2, \cdots h_\nu}) = z_{h_1, \cdots h_\alpha + \lambda, \cdots h_\beta + \mu, \cdots h_\nu},$$
$$\Theta_\alpha^{(\lambda)} \Theta_\beta^{(\mu)} (z_{h_1, h_2, \cdots h_\nu}) = \Theta_\beta^{(\mu)} \Theta_\alpha^{(\lambda)} (z_{h_1, h_2, \cdots h_\nu}).$$

Die Θ sind nach ihrer ersten oben abgeleiteten Eigenschaft durch eine beliebige cyklische Function rational darstellbar. Betrachtet man also die cyklischen Functionen der Wurzeln von $\mathfrak{F}(z) = 0$ als bekannt, d. h. setzt man fest, dass sie im Rationalitätsbereiche vorkommen sollen, so fällt $\mathfrak{F} = 0$ unter die in § 503 definirten Gleichungen, d. h. $\mathfrak{F}(z) = 0$ ist eine Abel'sche Gleichung. Demgemäss kann man die Abelschen Gleichungen auch folgendermassen definiren: $\mathfrak{F}(z) = 0$ ist eine Abel'sche Gleichung, wenn ihre Wurzeln nach ν Dimensionen so angeordnet werden können, dass die hiernach als cyklisch zu charakterisirenden Functionen derselben im festgesetzten Rationalitätsbereiche enthalten sind*).

*) Vgl. hier und für das Folgende: Kronecker l. c.

Von der früheren Definition können wir umgekehrt zur jetzigen kommen. Bildet man nämlich nach § 509 zu den Elementen $\Theta(\zeta)$ eine Basis $\Theta_1, \Theta_2, \cdots \Theta_r$ und setzt für die Exponenten $h_1, h_2, \cdots h_r$, welche das Element Θ charakterisiren, die Bezeichnung an

$$\Theta = \Theta_1^{h_1} \Theta_2^{h_2} \cdots \Theta_r^{h_r}(\zeta) \equiv \zeta_{h_1, h_2, \cdots h_r},$$

so ist eine erweiterte cyklische Anordnung der Wurzeln erreicht. Hierbei gelangt man auch zu der kleinsten Anzahl r der einzuführenden Indices; r heisse der **Rang der Abel'schen Gleichung** (vgl. § 509 und § 513). Cyklische Gleichungen im engeren Sinne haben den Rang 1.

§ 528. Jede rationale Function von Wurzeln beliebig vieler Abel'scher Gleichungen des Rationalitätsbereiches ist Wurzel einer Abel'schen Gleichung (vgl. § 498). Dies folgt unmittelbar aus der obigen Definition, wenn man die festgelegte rationale Function der Wurzeln Abel'scher Gleichungen durch die Gesammtheit der verschiedenen Indices charakterisirt, welche die einzelnen Wurzeln der Gleichungen kennzeichnen, d. h. wenn man etwa

$$f(\xi_{h_1, h_2, \cdots}, \eta_{k_1, k_2, \cdots}, \zeta_{l_1, l_2, \cdots}, \cdots) = \varrho_{h_1, h_2, \cdots; k_1, k_2, \cdots; l_1, l_2, \cdots}$$

setzt, wobei die ξ die Wurzeln der einen Abel'schen Gleichung sind, die η die Wurzeln einer anderen u. s. f., und wobei f die gegebene rationale Function der Argumente ist.

Umgekehrt kann jede Wurzel einer Abel'schen Gleichung höheren Ranges als rationale Function von Wurzeln cyklischer Gleichungen dargestellt werden.

Dies wollen wir derart beweisen, dass wir zuerst

$$z_{h_1, h_2, \cdots h_\nu} \qquad (h_\alpha = 1, 2, \cdots n_\alpha)$$

als rationale Function der Summen

$$(18) \qquad \sum_{k_2, k_3, \cdots} z_{k_1, k_2, k_3, \cdots}, \quad \sum_{k_1, k_3, \cdots} z_{k_1, k_2, k_3, \cdots}, \quad \cdots \qquad (k_\alpha = 1, 2, \cdots n_\alpha)$$

darstellen, deren Coefficienten cyklische Functionen der N Grössen z sein sollen. Wir bezeichnen jene Summe mit

$$\zeta_{k_1}^{(1)}, \quad \zeta_{k_2}^{(2)}, \quad \cdots$$

und betrachten die Producte

$$\zeta_{k_1}^{(1)} \zeta_{k_2}^{(2)} \cdots \zeta_{k_r}^{(\nu)} = \xi_{k_1, k_2, \cdots k_\nu}.$$

Wendet man hierauf die Substitution

$$(12) \qquad s_\mu = \left| z_{h_1, \cdots h_\mu, \cdots h_\nu} \quad z_{h_1, \cdots h_\mu + 1, \cdots h_\nu} \right|$$

an, dann ändert sich dabei von den ζ nur dasjenige, dessen Index k_μ

ist, da die übrigen Summen sich nur cyklisch in sich verschieben; dagegen geht ζ_{k_μ} in $\zeta_{k_\mu+1}$ über, und also entspricht der Substitution (12) zwischen den z die folgende zwischen den ξ

$$\sigma_\mu = \left| \xi_{h_1, \cdots h_\mu, \cdots h_\nu} \quad \xi_{h_1, \cdots h_\mu + 1, \cdots h_\nu} \right|.$$

Wir können daher die an (17) geknüpften Schlüsse hier bei der Gleichung

$$(19) \quad z_{h_1, h_2, \cdots h_\nu} = \sum_{k_1, k_2, \cdots} B_{k_1, k_2, \cdots} \xi_{h_1+k_1, h_2+k_2, \cdots} \qquad (k_\alpha = 1, 2, \cdots n_\alpha)$$

wiederholen und erkennen, dass die B cyklische Functionen der z werden oder unter den cyklischen Functionen stehen; sie gehören zu den bekannten Grössen. Auch hinsichtlich der Determinante

$$\varDelta = \left| \xi_{h_1+k_1, h_2+k_2, \cdots} \right|$$

gelten die früheren Schlüsse, indem man durch passende Combination solcher Zeilen, in denen z. B. h_1 allein geändert wird, eine Zerlegung von $\varDelta$ in lineare Factoren

$$\varDelta = \text{const.} \prod_{\alpha, \varkappa} \left(\sum_\lambda \omega_\alpha^{\lambda \varkappa} \zeta_\lambda^{(\varkappa)} \right)^{N : n_\alpha} \qquad \left(\omega_\alpha^{n_\alpha} = 1 \right)$$

erreichen kann; die Constante verschwindet dabei nicht. Es ist also für unbestimmte z die Determinante von Null verschieden.

Mit der Darstellung (19) von $z_{h_1, h_2, \cdots h_\nu}$ durch die Grössen (18) ist aber die Behauptung erwiesen. Denn es sind alle Grössen $\zeta_1^{(\alpha)}, \zeta_2^{(\alpha)}, \cdots \zeta_{n_\alpha}^{(\alpha)}$ Wurzeln einer cyklischen Gleichung, und die Coefficienten dieser Gleichung sind in allen Indices symmetrische Functionen der $z_{k_1, k_2, \cdots k_\nu}$ und gehören also zu den rational bekannten Grössen.

Damit ist gezeigt, dass es ausreicht, statt der Wurzeln allgemeiner Abel'scher Gleichungen solche der einfacheren cyklischen Gleichungen zu untersuchen.

Dreiundfünfzigste Vorlesung.

Die lineare Gruppe.

§ 529. Wir haben erwähnt, dass Cauchy die allgemeinen cyklischen Substitutionen mit dem Namen der arithmetischen belegt hat (§ 524). Ihnen stellt er dann die geometrischen Substitutionen gegenüber. Mit diesen wollen wir uns jetzt beschäftigen.

Zwischen den $N = n_1 \cdot n_2 \cdots n_\nu$ Grössen

$$z_{h_1, h_2, \cdots h_\nu} \qquad (h_\alpha = 1, 2, \cdots n_\alpha)$$

sei eine Substitution durch das Symbol

$$(1) \qquad t = | z_{h_1, h_2, \cdots h_\nu} \quad z_{a_1 h_1 + b_1 h_2 + \cdots + c_1 h_\nu,\, a_2 h_1 + b_2 h_2 + \cdots + c_2 h_\nu, \cdots} |,$$

oder kürzer bei blosser Angabe der Indicesumwandlung durch

$$(1^a) \qquad t = | h_\varkappa \quad a_\varkappa h_1 + b_\varkappa h_2 + \cdots + c_\varkappa h_\nu | \qquad (\varkappa = 1, 2, \cdots \nu)$$

definirt, bei welcher jeder Index h_α durch seinen kleinsten positiven Rest mod. n_α zu ersetzen ist. Diese heisst eine **geometrische Substitution**. Der Einfachheit halber wollen wir alle $n_1, n_2, \cdots n_\nu$ einander gleich und gleich n nehmen.

Nicht für jede Wahl der $a, b, \cdots c$ stellt dann (1) eine Substitution dar. So führt das Symbol

$$t = | h_1, h_2 \quad 2h_1 + h_2, h_1 + 2h_2 | \qquad (n = 3)$$

die neun Grössen, welche durch z_{h_1, h_2} für $h_1, h_2 = 1, 2, 3$ definirt werden,

$$z_{11}, \; z_{12}, \; z_{13}, \; z_{21}, \; z_{22}, \; z_{23}, \; z_{31}, \; z_{32}, \; z_{33}$$

in die Grössen

$$z_{33}, \; z_{12}, \; z_{21}, \; z_{21}, \; z_{33}, \; z_{12}, \; z_{12}, \; z_{21}, \; z_{33}$$

über; t ist also keine Substitution der neun Grössen, da es dieselben nicht permutirt, sondern zu je dreien immer in einen Werth umwandelt.

Es muss, um eine Substitution zu charakterisiren, im allgemeinen Falle dafür gesorgt werden, dass alle die n^ν verschiedenen Systeme $h_1, h_2, \cdots h_\nu$ durch t wieder in lauter verschiedene, d. h. wieder in alle n^ν verschiedenen Systeme übergeführt werden. Es dürfen demgemäss $h_1', h_2', \cdots h_\nu'$ und $h_1'', h_2'', \cdots h_\nu''$ nur dann die gleiche Umwandlung erleiden, wenn $h_1' \equiv h_1''$, $h_2' \equiv h_2''$, $\cdots$ ist. Setzt man $h_1' - h_1'' = k_1$, $h_2' - h_2'' = k_2, \cdots$, dann muss somit aus den linearen Congruenzen

$$(2) \qquad \begin{aligned} a_1 k_1 + b_1 k_2 + \cdots + c_1 k_\nu &\equiv 0, \\ a_2 k_1 + b_2 k_2 + \cdots + c_2 k_\nu &\equiv 0, \\ \cdots\cdots\cdots\cdots & \\ a_\nu k_1 + b_\nu k_2 + \cdots + c_\nu k_\nu &\equiv 0 \end{aligned} \quad (\text{mod. } n)$$

mit Nothwendigkeit folgen $k_1 \equiv 0$, $k_2 \equiv 0, \cdots$.

Bezeichnet man mit Δ die Determinante der $a, b, \cdots c$, so wird

$$\Delta k_1 \equiv 0, \quad \Delta k_2 \equiv 0, \quad \cdots \quad \Delta k_\nu \equiv 0 \quad (\text{mod. } n).$$

Unsere Forderung wird deshalb stets dann und nur dann befriedigt sein, wenn Δ nicht $\equiv 0$ (mod. n) ist. **Dafür, dass (1) eine geo-**

metrische Substitution darstellt, ist es charakteristisch, dass die Determinante Δ der Coefficienten mit dem Modul n keinen Theiler gemeinsam hat.

§ 530. Wendet man nach Benutzung von (1) auf das Resultat eine andere geometrische Substitution

$$t' = |h_x \quad a'_x h_1 + b'_x h_2 + \cdots + c'_x h_\nu| \qquad (x = 1, 2, \cdots \nu)$$

an, so entsteht

$$tt' = |h_x \quad (a'_x a_1 + b'_x a_2 + \cdots + c'_x a_\nu) h_1 + (a'_x b_1 + b'_x b_2 + \cdots + c'_x b_\nu) h_2 + \cdots|.$$

Das Resultat hat also die Form einer geometrischen Substitution; und da seine Determinante gleich dem Producte der Determinante von t und der von t' ist, so wird auch das Product tt' wirklich wieder eine geometrische Substitution und zwar eine eindeutig bestimmte.

Man überzeugt sich leicht davon, dass $(tt')t'' = t(t't'')$ ist.

Setzt man $t' = t$, so erhält man t^2; durch weitere „Multiplication" mit t entsteht t^3, u. s. w. Wenden wir auf die Reihe $t, t^2, t^3, \cdots$ die bekannten Schlussfolgerungen an, so zeigt sich, dass eine erste Potenz t^m besteht, welche jeden Index h in sich selbst umwandelt, so dass also t^m die Determinante besitzt

$$\begin{vmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix} \quad (\text{mod. } n).$$

Mit ihrer Hülfe können dann die negativen Potenzen

$$t^{-1} = t^{m-1}, \quad t^{-2} = t^{m-2}, \ \cdots$$

definirt werden. Uebrigens lässt sich t^{-1} auch als diejenige Substitution, welche die Wirkung von t wieder aufhebt, direct bestimmen, falls man

$$t^{-1} = |h_x \quad \alpha_x h_1 + \beta_x h_2 + \cdots + \gamma_x h_\nu|$$

ansetzt und die Coefficienten $\alpha, \beta, \cdots \gamma$ aus den ν^2 Congruenzen berechnet, die durch

$$(3) \qquad \begin{vmatrix} \alpha_1 \beta_1 \cdots \gamma_1 \\ \alpha_2 \beta_2 \cdots \gamma_2 \\ \cdot \ \cdot \ \cdot \ \cdot \end{vmatrix} \cdot \begin{vmatrix} a_1 b_1 \cdots c_1 \\ a_2 b_2 \cdots c_2 \\ \cdot \ \cdot \ \cdot \ \cdot \end{vmatrix} \equiv \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix} \quad (\text{mod. } n)$$

geliefert werden. Die $\alpha, \beta, \cdots$ bilden das zu den $a, b, \cdots$ reciproke System.

Hat man $tt' = tt''$ oder $t't = t''t$, dann liefert die linksseitige oder die rechtsseitige Multiplication mit t^{-1} das Resultat $t' = t''$.

Es sind also alle Bedingungen für eine Gruppe durch die t erfüllt. Wir wollen die Gruppe der t die geometrische Gruppe nennen.

§ 531. Um die Ordnung der geometrischen Gruppe festzustellen, brauchen wir ein Hülfstheorem.

Jedes System von ν Coefficienten $a_1, b_1, \cdots c_1$, welches einer geometrischen Substitution angehört, ist so beschaffen, dass der grösste gemeinsame Theiler q seiner Elemente theilerfremd zu n ist. Umgekehrt können zu jedem System $a_1, b_1, \cdots c_1$, dessen grösster gemeinsamer Theiler zu n theilerfremd ist, andere $(\nu - 1)$ Zeilen bestimmt werden

$$(4) \qquad \begin{matrix} a_1 & b_1 & \cdots & c_1 \\ u_1 & u_2 & \cdots & u_\nu \\ v_1 & v_2 & \cdots & v_\nu \\ \cdot & \cdot & \cdot & \cdot \\ w_1 & w_2 & \cdots & w_\nu, \end{matrix}$$

so dass das Schema als System der Coefficienten einer geometrischen Substitution genommen werden kann, indem die Determinante von (4) $\equiv q \pmod{n}$ gemacht wird. Am einfachsten lässt sich dieser Satz folgendermassen ableiten*). Wir zerlegen n in seine Primzahlpotenzen $p_1^{\varkappa_1} p_2^{\varkappa_2} \cdots$; dann ist sicher eine der Zahlen $a_1, b_1, \cdots c_1$ zu p_1 theilerfremd z. B. a_1. Bei der Entwickelung der Determinante von (4) möge nun ein Glied $a_1 u_\alpha v_\beta \cdots w_\gamma$ auftreten; dann setzen wir

$$a_1 u_\alpha \equiv q; \quad v_\beta \equiv 1; \quad \cdots \quad w_\gamma \equiv 1 \quad (\text{mod.}\, p_1^{\varkappa_1}),$$

und nach demselben Modul alle übrigen Elemente $u, v, \cdots w$ congruent 0. In gleicher Weise verfahren wir mit $p_2^{\varkappa_2}, \cdots$. So erhalten wir eine Reihe von Congruenzsystemen. Diese sind lösbar, da jedes einzelne System jedes $u, v, \cdots w$ nur einmal enthält, und da die verschiedenen Systeme zu theilerfremden Moduln gehören. Die Lösung führt auf $\Delta \equiv q$ (mod. $p_1^{\varkappa_1}$), (mod. $p_2^{\varkappa_2}$), $\cdots$ und also auf

$$\Delta \equiv q \quad (\text{mod.}\, n).$$

Damit ist die Möglichkeit erwiesen. —

Unter dem Symbole $[n, \nu]$ wollen wir nun die Anzahl der Möglichkeiten verstehen, ν ganze Zahlen $a_1, b_1, \cdots c_1$ so zu wählen, dass ihr grösster gemeinsamer Theiler zu n theilerfremd ist. Um diese Anzahl zu berechnen, nehmen wir zunächst alle überhaupt möglichen Systeme von ν Zahlen (mod. n), also n^ν, wobei wieder $n = p_1^{\varkappa_1} p_2^{\varkappa_2} \cdots$ sein soll. Von diesen Systemen sind alle diejenigen auszuschliessen, deren Elemente sämmtlich durch p_1 theilbar werden, das heisst $\left(\frac{n}{p_1}\right)^\nu$; ebenso

*) Frobenius, Journ. f. Math. 88 (1880), p. 97.

sind diejenigen auszuschliessen, deren Elemente sämmtlich durch p_2 theilbar sind, d. h. $\left(\frac{n}{p_2}\right)^\nu$; u. s. w. Nun folgen die bekannten Schlüsse, aus denen sich ergiebt, dass die Anzahl der gesuchten Systeme

$$(5)\qquad \begin{aligned}[n, \nu] &= n^\nu - \left(\frac{n}{p_1}\right)^\nu - \left(\frac{n}{p_2}\right)^\nu - \cdots + \left(\frac{n}{p_1 p_2}\right)^\nu + \cdots - \left(\frac{n}{p_1 p_2 p_3}\right)^\nu - \cdots \\ &= n^\nu\left(1 - \frac{1}{p_1^\nu}\right)\left(1 - \frac{1}{p_2^\nu}\right) \cdots\end{aligned}$$

beträgt.

Im Falle, dass n eine Primzahl wird, ergiebt sich das Resultat

$$(5^a)\qquad [p, \nu] = p^\nu - 1.$$

Nach diesen Vorbereitungen ist es leicht, die Ordnung der geometrischen Gruppe zu bestimmen. Wir setzen diese gesuchte Zahl, welche die Ordnung angiebt, gleich $\Phi(n, \nu)$.

Es seien zunächst alle diejenigen geometrischen Substitutionen

$$\tau_1, \quad \tau_2, \quad \tau_3, \cdots \tau_\varrho$$

herausgehoben, die den ersten Index h_1 in (1) ungeändert lassen.

Ist dann t_1 eine Substitution (1), welche h_1 in $a_1 h_1 + a_1 h_2 + \cdots + c_1 h_\nu$ umwandelt, dann thun dies auch alle Substitutionen

$$t_1\tau_1, \quad t_1\tau_2, \quad t_1\tau_3, \cdots t_1\tau_\varrho$$

und nur sie (vgl. die Schlüsse aus § 508, E). Jede geometrische Substitution wird also erhalten, wenn man alle Umwandlungsmöglichkeiten von h_1 aufzählt und eine jede mit der Gruppe aller τ verbindet.

Zur Art des t_1 gehört jede, bei der $a_1, b_1, \cdots c_1$ mit n keinen gemeinsamen Theiler besitzt. Folglich giebt es von der ersten Art nach dem oben Besprochenen im Ganzen $[n, \nu]$.

Ferner hat jedes τ die Form

$$| h_1, h_2, \cdots h_\nu \quad h_1, a_2 h_1 + b_2 h_2 + \cdots + c_2 h_\nu, \cdots a_\nu h_1 + b_\nu h_2 + \cdots + c_\nu h_\nu |;$$

man sieht, dass zu ihr die Determinante

$$(6)\qquad \begin{vmatrix} 1 & 0 & \cdots & 0 \\ a_2 & b_2 & \cdots & c_2 \\ a_3 & b_3 & \cdots & c_3 \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

gehört. Hieraus ersieht man, dass $a_2, a_3, \cdots a_\nu$ ganz beliebig gewählt werden können, während die Determinante

$$(7)\qquad \varDelta_1 = \begin{vmatrix} b_2 & \cdots & c_2 \\ b_3 & \cdots & c_3 \\ \cdot & \cdot & \cdot \end{vmatrix}$$

zu n theilerfremd sein muss. Es hat daher die Substitution

$$t' = | h_2, h_3, \cdots h_\nu \quad b_2 h_2 + \cdots + c_2 h_\nu, b_3 h_2 + \cdots + c_3 h_\nu, \cdots |$$

für $(\nu - 1)$ Indices dieselbe Bedeutung, wie t für ν Indices. Folglich ist die Anzahl der t' oder der Determinanten (7) gleich $\Phi(n, \nu - 1)$.

Somit wird die Ordnung der geometrischen Gruppe bei ν Indices und dem Modul n

$$\begin{aligned}\Phi(n, \nu) &= [n, \nu] n^{\nu-1} \Phi(n, \nu - 1) \\ &= [n, \nu] n^{\nu-1} [n, \nu - 1] n^{\nu-2} \cdots [n, 2] n^1 [n, 1].\end{aligned} \tag{8}$$

Für eine Primzahl $n = p$ wird dies einfach

$$\Phi(p, \nu) = (p^\nu - 1)(p^\nu - p)(p^\nu - p^2) \cdots (p^\nu - p^{\nu-1}). \tag{8^a}$$

Die hierbei benutzte Methode der Berechnung beruht darauf, dass jedes t, welches h_1 durch $a_1 h_1 + b_1 h_2 + \cdots + c_1 h_\nu$ ersetzt, durch das Product eines festen t gleicher Eigenschaft und eines τ dargestellt werden kann, wobei τ das h_1 nicht umstellt. Für das τ gilt dieselbe Reduction in Beziehung auf h_2, u. s. f.

Leicht können wir auch die Anzahl derjenigen geometrischen Substitutionen berechnen, deren Determinante modulo n congruent zu einer beliebigen Zahl q_0 ist; q_0 ist natürlich theilerfremd zu n anzunehmen. Wir gehen wie oben zur Bildung der gesuchten Substitutionen vor. Wir wählen auf $[n, \nu]$ Arten $a_1, b_1, \cdots c_1$; ihr grösster gemeinsamer Theiler sei q_1. Ferner wählen wir auf $[n, \nu - 1]$ Arten $b_2, \cdots c_2$; ihr grösster gemeinsamer Theiler sei q_2; u. s. f. bis zu $q_{\nu-1}$. Dann kann man stets ein letztes Element c_ν gemäss der Congruenz

$$q_1 q_2 \cdots q_{\nu-1} c_\nu \equiv q_0 \pmod{n}$$

bestimmen, und erhält also, wie auch $q_1, q_2, \cdots q_{\nu-1}$ angenommen waren, durch diese Wahl des c_ν eine passende Substitution. Bei diesem Vorgehen wird an der Bestimmung (8) nichts weiter geändert, als dass der letzte Factor $[n, 1] = \varphi(n)$ fortzulassen ist, d. h.: Der $\varphi(n)^{\text{te}}$ Theil aller geometrischen Substitutionen hat eine Determinante $\equiv 1 \pmod{n}$, und ebensoviele geometrische Substitutionen haben als Werth der Determinante eine willkürliche zu n theilerfremde Zahl (mod. n). Das gleiche Resultat hätte leicht auch so hergeleitet werden können, dass wir die Gleichheit der Anzahlen für alle diese einzelnen Classen nachgewiesen hätten.

Die geometrischen Substitutionen, deren Determinante $\equiv 1 \pmod{n}$ ist, bilden eine Untergruppe der geometrischen Gruppe, die in jeder aus geometrischen Substitutionen bestehenden Gruppe vorkommt.

Bilden μ zu n theilerfremde Zahlen $q_1, q_2, \cdots q_\mu$ insofern eine Gruppe, als das Product zweier unter ihnen $q_\alpha \cdot q_\beta$ wieder zum Systeme der q gehört, dann bilden auch alle zu den einzelnen Determinantenwerthen

$$\Delta \equiv q_1, \quad \equiv q_2, \quad \cdots \quad \equiv q_\mu \qquad (\text{mod. } n)$$

gehörigen geometrischen Substitutionen eine Gruppe. Dies findet insbesondere statt, wenn $q_1, q_2, \cdots q_\mu$ alle quadratischen Reste (mod. n) darstellen. Für $n = p$ wird $\mu = \frac{p-1}{2}$, und die so gebildete Gruppe enthält halb so viele Substitutionen als die gesammte geometrische Gruppe.

§ 532. Wir haben bereits bemerkt, dass die Determinante, welche aus den Coefficienten von (1ᵃ) gebildet wird, sich als wichtig für die Substitutionen ausweist. Wir wollen jetzt

$$(1^b) \qquad t = | h_\varkappa \quad a_{\varkappa 1} h_1 + a_{\varkappa 2} h_2 + \cdots + a_{\varkappa \nu} h_\nu | \qquad (\varkappa = 1, 2, \cdots \nu)$$

auch in der determinantenähnlichen Form

$$(1^c) \qquad t = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1\nu} \\ a_{21} & a_{22} & \cdots & a_{2\nu} \\ \cdot & \cdot & \cdot & \cdot \\ a_{\nu 1} & a_{\nu 2} & \cdots & a_{\nu\nu} \end{pmatrix} = (a_{ik}) \qquad (i, k = 1, 2, \cdots \nu)$$

schreiben und die elementaren Sätze über Determinanten mit Theoremen über unsere Substitutionen t in Verbindung bringen.

Zunächst überzeugt man sich durch wirkliche Ausrechnung sofort davon, dass wenn $t = (a_{ik})$, $u = (b_{ik})$ ist, dann wie bei Determinantenmultiplication

$$t \cdot u = (a_{ik}) \cdot (b_{ik}) = \Big(\sum_{(\lambda)} a_{i\lambda} b_{\lambda k}\Big)$$

wird.

Wir wollen ferner eine Anzahl besonders einfacher Determinanten oder Substitutionen in ihrer Wirkung auf t betrachten. Hier untersuchen wir zunächst

$$(9) \qquad v_{\alpha\beta} = (a_{ik}) \qquad (a_{\varkappa\varkappa} = 1;\ a_{\alpha\beta} = 1;\ \text{alle anderen } a_{ik} \text{ gleich } 0).$$

Es ist, wie eine leichte Rechnung zeigt,

$$(9^a) \qquad \begin{aligned} v_{\alpha\beta}\, t &= \begin{pmatrix} a_{11} & a_{12} & \cdots \\ \cdot & \cdot & \cdot \\ a_{\alpha 1} + a_{\beta 1} & a_{\alpha 2} + a_{\beta 2} & \cdots \\ \cdot & \cdot & \cdot \\ a_{\nu 1} & a_{\nu 2} & \cdots \end{pmatrix} \cdots \text{(die } \beta^{\text{te}} \text{ Zeile um die Elemente der } \alpha^{\text{ten}} \text{ vermehrt)}, \\ t\, v_{\alpha\beta} &= \begin{pmatrix} a_{11} & \cdots & a_{1\alpha} + a_{1\beta} & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ a_{\nu 1} & \cdots & a_{\nu\alpha} + a_{\nu\beta} & \cdots \end{pmatrix} \cdots \text{(die } \alpha^{\text{te}} \text{ Spalte um die Elemente der } \beta^{\text{ten}} \text{ vermehrt)}. \end{aligned}$$

Weiter betrachten wir die Determinante oder Substitution von der Gestalt

$$(10) \qquad w_{\alpha\beta} = (a_{ik})$$

$(a_{\varkappa\varkappa} = 1$ für alle $\varkappa$ ausser α, β; $a_{\alpha\beta} = a_{\beta\alpha} = 1$; alle anderen a_{ik} gleich $0)$.

Für sie erhält man

$$(10^a) \quad \begin{aligned} w_{\alpha\beta} t &= (a'_{ik}) \qquad (a'_{ik} = a_{ik}, \text{ ausser } a'_{\alpha k} = a_{\beta k} \text{ und } a'_{\beta k} = a_{\alpha k}), \\ t w_{\alpha\beta} &= (a'_{ik}) \qquad (a'_{ik} = a_{ik}, \text{ ausser } a'_{k\alpha} = a_{k\beta} \text{ und } a'_{k\beta} = a_{k\alpha}). \end{aligned}$$

Die Determinante oder Substitution

$$(11) \quad n_\alpha = (a_{ik}) \qquad (a_{\varkappa\varkappa} = 1, \text{ ausser } a_{\alpha\alpha} = -1; \text{ alle anderen } a_{ik} \text{ gleich } 0)$$

endlich ruft die Aenderungen hervor

$$(11^a) \quad \begin{aligned} n_\alpha t &= (a'_{ik}) \qquad (a'_{ik} = a_{ik}, \text{ ausser } a'_{\alpha k} = -a_{\alpha k}), \\ t n_\alpha &= (a'_{ik}) \qquad (a'_{ik} = a_{ik}, \text{ ausser } a'_{ik} = -a_{i\alpha}). \end{aligned}$$

Durch passende rechts- oder linksseitige Multiplication mit einer der Substitutionen

$$v_{\alpha\beta}, \quad w_{\alpha\beta}, \quad n_\alpha$$

sind wir also im Stande, jedes t in ein anderes umzuwandeln, bei welchem gegen das erste entweder zu einer Zeile (Spalte) die entsprechenden Elemente einer anderen Zeile (Spalte) addirt werden; oder bei welcher zwei Zeilen (Spalten) miteinander vertauscht werden; oder endlich, bei welchem alle Elemente einer Zeile (Spalte) mit dem Factor -1 multiplicirt werden.

Diese Umänderungen wollen wir als **elementare Transformationen** der Substitution t auffassen. Wir können uns offenbar dabei auf die Benutzung der $(\nu + 1)$ Substitutionen

$$(12) \qquad w_{12}, \; w_{13}, \; \cdots \; w_{1\nu}; \; v_{12}; \; n_1$$

beschränken, da die anderen elementaren Transformationen leicht aus diesen abgeleitet werden können.

Diese elementaren Transformationen wollen wir nun dazu verwenden, um t aus besonders einfachen Formen zusammenzusetzen*).

Irgend ein gegebenes t kann nämlich zuerst durch Vertauschung von Reihen oder Multiplication aller Elemente einer Reihe mit -1 so eingerichtet werden, dass sein erstes Element a_{11} positiv und nicht grösser als der absolute Werth irgend eines der von Null verschiedenen Elemente der Determinante ist. Kommt dann in der ersten Zeile oder Spalte ein Element vor, welches nicht ein ganzes Viel-

*) Kronecker, Journ. f. Math. 107 (1891), p. 135.

faches von a_{11} ist, dann kann man dies durch passende Verbindung mit der ersten Zeile oder Spalte bei Verwendung der Umwandlung durch $v_{\alpha\beta}$ in ein anderes positives von geringerem absoluten Betrag als a_{11} umwandeln. Dieses Element lässt sich dann an die erste Stelle bringen. Da jede solche Transformation den absoluten Betrag des ersten Elementes verringert, dieser aber nicht Null werden kann, so führt unser Verfahren zu einem t, in dem a_{11} positiv, $\leqq |a_{ik}|$ und ein Theiler aller übrigen Elemente a_{1k} und a_{i1} wird.

Dieses System kann man nun weiter durch elementare Transformationen der Form $v_{\alpha\beta}$ so umwandeln, dass mit Ausnahme von a_{11} alle a_{i1} und alle a_{1k} gleich Null werden. Kommt ferner in einer Reihe dieses reducirten Systems ein Element $a_{\lambda\mu}$ vor, das kein Vielfaches von a_{11} ist, so addirt man die betreffende Zeile zur ersten und erhält ein t, in dem a_{11} nicht Theiler aller a_{1k} ist; das so erhaltene t kann dann noch weiter nach demselben Schema reducirt werden. Man kommt so, da das neue a_{11} noch kleiner geworden ist, schliesslich zu einem t, in dem das erste Element positiv und Divisor aller übrigen ist, und zugleich alle Elemente der ersten Zeile und Spalte mit Ausnahme des ersten Elementes gleich Null sind.

Wenn man dann die gleichen Reductionen auf das System der zweiten, $\cdots$ ν^{ten} Spalten und Zeilen anwendet und so fort geht, dann erlangt man ein t, in welchem jedes Element ausserhalb der Diagonale gleich Null wird, jedes von Null verschiedene Diagonalglied Divisor des folgenden ist, und alle diese bis auf das letzte positiv sind. Ist, wie bei uns, die Determinante der Substitution von Null verschieden, dann sind auch die Diagonalglieder sämmtlich von Null verschieden. Ferner bleiben alle diese Ableitungen gültig, wenn man das System der Coefficienten nach dem Modul n betrachtet. So folgt:

Jede Substitution t lässt sich aus einer Diagonalsubstitution der angegebenen Beschaffenheit

$$d = \begin{pmatrix} a_{11} & 0 & 0 & \cdots \\ 0 & a_{22} & 0 & \cdots \\ 0 & 0 & a_{33} & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} = |h_\varkappa \quad a_{\varkappa\varkappa} h_\varkappa| \pmod{n}$$

in Verbindung mit den Substitutionen (12) darstellen.

Es ist klar, dass jede Substitution t das Index-System $h_1 = n$, $h_2 = n, \cdots h_\nu = n$ oder, was das Gleiche sagt, $h_1 = 0$, $h_2 = 0$, $\cdots h_\nu = 0$ und also $z_{00\ldots}$ ungeändert lässt. Bei einzelnen Substitutionen t können aber auch noch andere Elemente ungeändert bleiben. Dafür, dass (1^b) dies thue, ist nämlich nur nothwendig, dass die Congruenz

$$\begin{vmatrix} a_{11}-1 & a_{12} & \cdots \\ a_{21} & a_{22}-1 & \cdots \\ \cdot & \cdot & \cdot \end{vmatrix} \equiv 0 \pmod{n}$$

erfüllt sei. Die Bestimmung der Elemente selbst hängt dann von der Auflösung eines Systems von linearen Congruenzen modulo n ab. Für $\nu = 1$ ist $|h_1 \ \ h_1| = t_0$ die einzige Substitution, welche mehr Elemente als das Eine $z_{0,0,\ldots}$ ungeändert lässt, nämlich sämmtliche; t_0 ist die identische Substitution oder die Einheitssubstitution.

§ 533. Wir verbinden nun die arithmetischen Substitutionen

(13) $s = |h_\alpha \ \ h_\alpha + d_\alpha|$ $\quad(\alpha = 1, 2, \cdots \nu$; h_α wird mod. n reducirt)

mit den oben aufgestellten geometrischen (1) und bezeichnen die aus allen s und t bestehende Gruppe als die zu n gehörige lineare Gruppe. Entsprechend dieser Bezeichnung könnten wir die Gruppe der t auch wohl als die zu n gehörige lineare homogene Gruppe bezeichnen. Durch die s und t wird jeder Index h_α in einen solchen von der Gestalt

$$a_{\alpha 1}h_1 + a_{\alpha 2}h_2 + \cdots + a_{\alpha\nu}h_\nu + d_\nu \qquad (\alpha = 1, 2, \cdots \nu)$$

umgeändert, gleichgültig ob wir die Folge $s \cdot t$ oder $t \cdot s$ betrachten. Wir schreiben deshalb die linearen Substitutionen in der Form

(14) $u = |h_\alpha \ \ a_{\alpha 1}h_1 + a_{\alpha 2}h_2 + \cdots + a_{\alpha\nu}h_\nu + d_\alpha|$ $\quad (\alpha = 1, 2, \cdots \nu)$.

Untersucht man wieder, wann das Symbol (14) eine Substitution darstellen kann, so kommt man hinsichtlich der $a_{\alpha\beta}$ auf (2) und die daran geknüpften Folgerungen zurück. Für die Wahl der d_α bestehen keine Einschränkungen. So ergiebt sich als Ordnung der linearen Gruppe der Werth $n^\nu \Phi(n, \nu)$.

Bemerkenswerth ist das Verhalten der u gegenüber den s. Es gilt nämlich zunächst die Gleichung

(15) $$ts_\varkappa = s_\lambda t \quad \text{oder} \quad t^{-1}s_\lambda t = s_\varkappa,$$

wo bei gegebenem t entweder s_λ aus gegebenem $s_\varkappa$ oder umgekehrt $s_\varkappa$ aus gegebenem s_λ bestimmt werden kann. Um dies zu beweisen, setzen wir

$$s_\varkappa = |h_\alpha \ \ h_\alpha + d_\alpha|, \quad s_\lambda = |h_\alpha \ \ h_\alpha + q_\alpha|,$$
$$t = |h_\alpha \ \ a_{\alpha 1}h_1 + a_{\alpha 2}h_2 + \cdots + a_{\alpha\nu}h_\nu|,$$

und daraus ergeben sich die beiden Gleichungen

$$ts_\varkappa = |h_\alpha \ \ a_{\alpha 1}h_1 + \cdots + a_{\alpha\nu}h_\nu + (a_{\alpha 1}d_1 + \cdots + a_{\alpha\nu}d_\nu)|,$$
$$s_\lambda t = |h_\alpha \ \ a_{\alpha 1}h_1 + \cdots + a_{\alpha\nu}h_\nu + q_\alpha|;$$

es sind also je nach den Voraussetzungen die d durch die q oder umgekehrt die q durch die d vermittels des Gleichungssystems

$$a_{\alpha 1} d_1 + a_{\alpha 2} d_2 + \cdots + a_{\alpha \nu} d_\nu \equiv q_\alpha \qquad (\alpha = 1, 2, \cdots \nu)$$

zu bestimmen. Die Bestimmung der q ist selbstverständlich; und da die Determinante der a von Null verschieden ist, (mod. n) betrachtet, so ist auch umgekehrt die Bestimmung der d durch die q stets möglich.

Hiermit haben wir zugleich gezeigt, dass jedes u ersetzt werden kann durch ein Product

$$u = t s_\varrho = s_\sigma t,$$

in welchem das t in den Coefficienten $a_{\varkappa\lambda}$ mit u übereinstimmt, während die Substitutionen s_ϱ bezw. s_σ derart gewählt sind, wie die obigen Gleichungen es vorschreiben.

Daraus folgt dann weiter, dass man auch

$$(16) \qquad u s_\varkappa = s_\lambda u \quad \text{oder} \quad u^{-1} s_\lambda u = s_\varkappa$$

hat, wo bei gegebenem u entweder s_λ aus gegebenem $s_\varkappa$ oder umgekehrt $s_\varkappa$ aus gegebenem s_λ bestimmt werden kann. Die Form $u^{-1} s_\lambda u$ wird sich als besonders wichtig ausweisen (§ 541; 542).

§ 534. Wir wenden uns jetzt zu dem besonderen Falle, dass $\nu = 1$ und $n = p$ d. h. eine Primzahl ist. Dabei haben wir also die drei Formen zu beachten

$$\begin{aligned} s &= | z_h \quad z_{h+d} | \\ t &= | z_h \quad z_{ah} | \qquad (h = 1, 2, \cdots p). \\ u &= | z_h \quad z_{ah+d} | \end{aligned}$$

Alle s sind Potenzen der Substitution $s_0 = | z_h \; z_{h+1} |$, und alle t ebenso Potenzen der Substitution $t_0 = | z_h \; z_{gh} |$, wenn g eine primitive Wurzel mod. p bedeutet. Jedes u lässt sich in die Form $s_0^\alpha t_0^\beta$ oder $t_0^\gamma s_0^\delta$ bringen, so dass die Gruppe bereits durch s_0 und t_0 bestimmt ist. Die lineare Gruppe bezeichnen wir in diesem Falle nach Kronecker als metacyklische Gruppe. Ihre Ordnung ist gleich $p(p-1)$.

Lässt ein u zwei Elemente z ungeändert etwa z_h und z_k, so ist

$$\begin{aligned} ah + d \equiv h, \quad ak + d \equiv k \\ a(h-k) \equiv h - k \end{aligned} \qquad (\text{mod. } p),$$

und also, da $(h-k)$ nicht durch p theilbar ist, $a \equiv 1$; daraus folgt dann $d \equiv 0$. Dieses u, welches zwei Elemente nicht ändert, reducirt sich somit auf die Einheitssubstitution, d. h. es ändert überhaupt kein Element.

Lässt ein u hingegen kein Element z ungeändert, dann muss die Erfüllung der Congruenz

$$h(a-1)+d \equiv 0 \pmod{p}$$

für h unmöglich sein; a ist $\equiv 1 \pmod{p}$ und $d \not\equiv 0$, d. h. u gehört zu den arithmetischen Substitutionen.

In der metacyklischen Gruppe giebt es nur $(p-1)$ Substitutionen nämlich die arithmetischen s, welche alle Elemente umsetzen, und nur eine Substitution nämlich die Einheitssubstitution, welche mehr als ein Element und zwar alle ungeändert lässt. Die geometrischen Substitutionen $t = |h \quad g^a h|$ sind die einzigen, welche das Element z_0 nicht umstellen.

Weitere Untersuchungen über die metacyklische Gruppe werden wir später in der Vorlesung über auflösbare Gleichungen eines Primzahlgrades anstellen.

Eine metacyklische Function heisst jede solche, welche bei den Substitutionen der metacyklischen Gruppe und nur bei ihnen ungeändert bleibt. Eine solche ist z. B., wenn g wieder eine primitive Congruenzwurzel mod. p bedeutet,

$$\varphi = \sum_{d=0}^{p-1} z_d^3 \left(z^2_{g^0+d} z_{g^1+d} + z^2_{g^1+d} z_{g^2+d} + \cdots + z^2_{g^{p-2}+d} z_{g^0+d} \right).$$

Denn erstens verschiebt $s_0 = |h \quad h+1|$ nur die einzelnen Glieder der Summe Σ cyklisch. Zweitens wandelt $t_0 = |h \quad gh|$ den hingeschriebenen Summanden aus Σ in

$$z^3_{dg} \left(z^2_{g^1+dg} z_{g^2+dg} + \cdots + z^2_{g^0+dg} z_{g^1+dg} \right)$$

um; und da mit d zugleich dg alle Zahlen $0, 1, \cdots (p-1)$ durchläuft, so bleibt φ auch für t_0 ungeändert. Nun kann jedes u, wie oben gezeigt wurde, aus s_0 und t_0 in der Form $u = s_0^\alpha t_0^\beta$ gebildet werden; folglich bleibt φ unter dem Einflusse der metacyklischen Gruppe ungeändert.

Wenn umgekehrt eine Substitution σ die Function φ nicht ändert, und wenn durch σ das Element z_0 in z_d umgewandelt wird, dann muss, wie die Bildung von φ zeigt, der gesammte Summand

$$z_0^3 \left(z^2_{g^0} z_{g^1} + z^2_{g^1} z_{g^2} + \cdots \right) \quad \text{in} \quad z_d^3 \left(z^2_{g^0+d} z_{g^1+d} + z^2_{g^1+d} z_{g^2+d} + \cdots \right)$$

übergeführt werden. Geht dabei z_{g^0} in $z_{g^\alpha+d}$ über, dann zeigt die Form des Summanden, dass zugleich z_{g^1} in $z_{g^{\alpha+1}+d}$, ferner z_{g^2} in

$z_{g^{\alpha+2}+d}$ u. s. f. umgewandelt werden muss. Demgemäss haben wir jene Substitution

$$\sigma = |z_h \quad z_{g^\alpha h+d}|$$

als Substitution der metacyklischen Gruppe erkannt.

Es ist klar, dass wir in φ die Exponenten 3, 2, 1 durch irgend welche von einander verschiedene ganze Zahlen ersetzen können.

§ 535. Wir betrachten nun eine cyklische zu $s_0 = |h \quad h+1|$ gehörige Function, d. h. eine solche, die sich nicht ändert, wenn z_0, $z_1, \cdots z_{p-1}$ cyklisch verschoben werden; wir bezeichnen sie

$$C(z_0, z_1, \cdots z_{p-1}) = C_0.$$

Dabei setzen wir fest, dass C nicht unter den cyklischen Functionen steht, also nicht für weitere Substitutionen ungeändert bleiben soll. Das C mag durch Verwendung der geometrischen Substitutionen

$$t_0 = |h \quad gh|, \quad t_0^2 = |h \quad g^2h|, \quad \cdots \quad t_0^{p-2} = |h \quad g^{p-2}h|$$

der Reihe nach in die Formen

$$C(z_0, z_g, z_{2g}, \cdots) = C_1, \quad C(z_0, z_{g^2}, z_{2g^2}, \cdots) = C_2, \quad \cdots$$
$$C(z_0, z_{g^{p-2}}, \cdots) = C_{p-2}$$

übergehen. Dann wird C_1 für $s = |h \quad h+g| = s_0^g$ ungeändert bleiben und also auch für $s_0^{2g}, s_0^{3g}, \cdots$. In dieser Reihe befindet sich aber s_0 selbst, da ja die Gesammtheit der Exponenten $g, 2g, 3g, \cdots$ für den Modul p mit $1, 2, 3, \cdots$ übereinstimmt. Mithin bleibt C_1 für dieselben Substitutionen ungeändert wie C_0. Das Gleiche gilt für die übrigen C_λ. Alle Werthe $C_0, C_1, \cdots C_{p-2}$ bleiben für die Potenzen von s_0 und nur für diese ungeändert.

Wir bilden nun eine cyklische Function der $C_0, C_1, \cdots C_{p-2}$ in der hingeschriebenen Anordnung genommen, also etwa, wenn ω eine primitive $(p-1)^{\text{te}}$ Einheitswurzel bedeutet, die Lagrange'sche Resolvente

$$(C_0 + \omega C_1 + \omega^2 C_2 + \cdots + \omega^{p-2} C_{p-2})^{p-1};$$

dann ist dies eine metacyklische Function der $z_0, z_1, \cdots z_{p-1}$, weil ja t_0 die einzelnen C cyklisch verschiebt, und s_0 sie ungeändert lässt. —

Jetzt möge eine Gleichung p^{ten} Grades

$$(15) \qquad f(z) \equiv (z-z_0)(z-z_1)(z-z_2)\cdots(z-z_{p-1}) = 0$$

von der Art vorgelegt sein, dass man den Wurzeln z_λ eine Anordnung geben kann, in welcher ihre metacyklischen Functionen dem Rationalitätsbereiche angehören. Eine solche Gleichung soll eine meta-

cyklische Gleichung heissen. Dann sind für diese Gleichung die cyklischen Functionen $C_0, C_1, \cdots C_{p-2}$ die Wurzeln einer Abel'schen Gleichung.

Denn setzt man die Gleichung an, von welcher $C_0, C_1, \cdots C_{p-2}$ als Wurzeln abhängen,

$$(16) \qquad G(v) \equiv (v - C_0)(v - C_1) \cdots (v - C_{p-2}) = 0,$$

so sind die Coefficienten von G als symmetrische Functionen der C unter den cyklischen enthalten und somit durch die metacyklischen Functionen der z ausdrückbar, d. h. rational bekannt. Ferner wird aus der Relation

$$G(v)\left[\frac{C_\alpha}{v - C_0} + \frac{C_{\alpha+1}}{v - C_1} + \frac{C_{\alpha+2}}{v - C_2} + \cdots\right] = H(v)$$

wie gewöhnlich erschlossen, dass die rationalen Beziehungen

$$C_\alpha = \psi_\alpha(C_0), \quad C_{\alpha+1} = \psi_\alpha(C_1), \quad C_{\alpha+2} = \psi_\alpha(C_2), \cdots$$

bestehen; für $\alpha = 1$ folgt, dass alle C_λ in C_0 rational sind; endlich ergiebt sich, wenn man in $C_\alpha = \psi_\alpha(C_0)$ das C_0 durch $C_\beta = \psi_\beta(C_0)$ und also C_α durch $C_{\alpha+\beta}$ ersetzt,

$$C_{\alpha+\beta} = \psi_\alpha[\psi_\beta(C_0)] = \psi_\beta[\psi_\alpha(C_0)].$$

Damit ist gezeigt, dass $G(v) = 0$ eine Abel'sche Gleichung ist.

Ist diese Abel'sche Gleichung aufgelöst, oder auch nur eine ihrer Wurzeln bestimmt, dann sind alle C bekannt; (15) ist dadurch also auf eine Abel'sche Gleichung reducirt und sonach (vgl. § 503) auflösbar. Die Auflösung der metacyklischen Gleichung (15) des Primzahlgrades p lässt sich durch die Auflösung zweier Abel'scher Gleichungen vollziehen, deren eine vom Grade p und deren andere vom Grade $(p-1)$ ist. Es werden in den nächsten Vorlesungen noch wichtige Bemerkungen zu diesem Satze herzuleiten sein, durch den wir hinsichtlich der Auflösbarkeit der Gleichungen über die Abel'schen oder allgemeinen cyklischen Gleichungen hinausgelangt sind.

§ 536. Eine Untergruppe der metacyklischen Gruppe wird durch die Substitutionen

$$v = |\, h \quad g^{2\varkappa} h + d \,| \qquad \left(h, d = 1, 2, \cdots p;\ \varkappa = 1, 2, \cdots \tfrac{1}{2}(p-1)\right)$$

gebildet. Aus unseren früheren Betrachtungen erkennt man sofort, dass die Ordnung der Gruppe $\frac{1}{2}p(p-1)$ wird; sie heisst nach Kronecker die halbmetacyklische Gruppe. Der Coefficient $g^{2\varkappa}$

von h durchläuft die Reihe der quadratischen Reste mod. p. Eine zu der Gruppe gehörige Function ist z. B.

$$\psi = \sum_{d=0}^{p-1} z_d^4 \left(z^3_{g^0+d} z^2_{g^1+d} z_{g^2+d} + z^3_{g^2+d} z^2_{g^3+d} z_{g^4+d} + \cdots \right).$$

Für $p = 5$ ist in der Schreibweise von § 522 die metacyklische Gruppe, falls nur die Indices in die Cyklen gesetzt werden,

1	(14) (23)	(1243)	(1342)
(01234)	(04) (13)	(0132)	(0324)
(02413)	(03) (12)	(0423)	(0143)
(03142)	(02) (34)	(0132)	(0412)
(04321)	(01) (24)	(0341)	(0231),

und die ersten beiden Spalten geben ihre halbmetacyklische Untergruppe.

§ 537. Nach der Untersuchung der Substitutionen von der Form $|z_h \;\; z_{ah}|$ wollen wir zu denjenigen der homogenen, linearen Substitutionen mit zwei Indices

$$|\, z_{h,k} \quad z_{ah+bk,\, a'h+b'k} \,| \qquad (h, k = 1, 2, \cdots p)$$

oder kürzer

$$(17) \qquad |\, h, k \quad ah + bk,\, a'h + b'k \,| \qquad (h, k = 1, 2, \cdots p)$$

übergehen, in denen alle Indices nach dem Modul p auf ihre kleinsten positiven Reste zu reduciren sind. Unsere Untersuchung soll sich auf die Frage nach der Ordnung solcher Substitutionen erstrecken, die wir als **binäre Substitutionen für den Modul** p bezeichnen.

Wir suchen zunächst zu entscheiden, ob es eine lineare Function $(mh + nk)$ giebt, welche durch (17) in eins ihrer Vielfachen $\varrho(mh + nk)$ übergeführt wird. Durch (17) geht der Ausdruck

$$mh + nk \quad \text{in} \quad (am + a'n)h + (bm + b'n)k$$

über; dies wird gleich $\varrho(mh + nk)$, falls das System der Congruenzen

$$(18) \qquad \begin{aligned} m(a - \varrho) + na' &\equiv 0 \\ mb + n(b' - \varrho) &\equiv 0 \end{aligned} \quad (\text{mod. } p)$$

erfüllt ist. Weil sich hieraus die quadratische Congruenz für ϱ

$$(19) \qquad \varrho^2 - \varrho(a + b') + (ab' - a'b) \equiv 0 \quad (\text{mod. } p)$$

ergiebt, so folgt, dass reelle unserer Forderung entsprechende ϱ nur dann existiren, wenn die Discriminante von (19)

$$D = (a + b')^2 - 4(ab' - a'b) = (a - b')^2 + 4a'b$$

quadratischer Rest von p ist. Zu bemerken bleibt noch, dass $(ab'-a'b)$ nicht congruent 0 (mod. p) werden kann, weil sonst (17) keine Substitution wäre (§ 529).

Wir haben also die drei Fälle zu unterscheiden: I) dass D ein quadratischer Rest für p ist; II) dass D durch p theilbar wird und III) dass D quadratischer Nichtrest für p ist. Diesen drei Fällen entsprechend sind entweder zwei reelle von einander verschiedene, oder es ist ein reeller, oder endlich kein reeller Werth für ϱ vorhanden.

Wir behandeln an erster Stelle das Problem unter der Annahme I), dass ϱ_1 und ϱ_2 zwei reelle, von einander verschiedene Werthe sind, die (19) befriedigen. Dann giebt es auch zwei reelle Systeme m_1, n_1 und m_2, n_2, welche Wurzeln von (18) für $\varrho=\varrho_1$ und $\varrho=\varrho_2$ sind; und setzen wir, um abzukürzen,

$$h_1 = m_1 h + n_1 k, \quad k_1 = m_2 h + n_2 k,$$

dann gehen durch (17) h_1 und k_1 in $h_1\varrho_1$ und $k_1\varrho_2$ über. Da man ferner als Auflösung der Congruenzen (18)

$$\begin{matrix} m_1 = \sigma a'; & n_1 = \sigma(\varrho_1 - a) \\ m_2 = \tau a'; & n_2 = \tau(\varrho_2 - a) \end{matrix} \quad \text{(mit beliebigen ganzzahligen } \sigma, \tau)$$

oder auch

$$\begin{matrix} m_1 = \sigma_1(\varrho_1 - b'); & n_1 = \sigma_1 b \\ m_2 = \tau_1(\varrho_2 - b'); & n_2 = \tau_1 b \end{matrix} \quad \text{(mit beliebigen ganzzahligen } \sigma_1, \tau_1)$$

setzen kann, so folgt, da $a'b \not\equiv 0$ ist, dass die Determinante

$$m_1 n_2 - m_2 n_1 = \sigma\tau a'(\varrho_2 - \varrho_1) = \sigma_1\tau_1 b(\varrho_2 - \varrho_1)$$

von Null verschieden ist, und deshalb, dass h und k linear durch h_1 und k_1 ausgedrückt werden können; d. h. also, man kann an Stelle von h und k auch h_1 und k_1 als neue Indices der z annehmen.

Wenn wir nun der bequemeren Bezeichnung wegen statt h_1, k_1 wieder h, k eintragen, so erhalten wir eine für diesen ersten Fall gültige Normalform

$$(17^a) \qquad u \equiv | h, k \quad \varrho_1 h, \varrho_2 k | \quad (\text{mod.}\, p).$$

Es ist hierbei

$$u^2 \equiv | h, k \quad \varrho_1^2 h, \varrho_2^2 k | \quad (\text{mod.}\, p).$$

Weil jede reelle Zahl ϱ in die $(p-1)^{\text{te}}$ Potenz erhoben $\equiv 1$ (mod. p) wird, so ist sicher $u^{p-1} \equiv 1$ (mod. p). Daraus schliessen wir in bekannter Weise, dass die Ordnung jedes u ein Theiler von $(p-1)$ sein muss.

Auf die Ableitung der Anzahl derjenigen binären Substitutionen, die zu einem bestimmten Exponenten gehören, wollen wir nicht eingehen; es mag genügen, das ohne Schwierigkeit herzuleitende Resultat anzugeben. Ist $q_1^{\nu_1} q_2^{\nu_2} q_3^{\nu_3} \cdots$ ein in seine Primfactor-Potenzen zerlegter Theiler von $(p-1)$, so gehören zu ihm

$$(q_1^{2\nu_1}-1)(q_2^{2\nu_2}-1)(q_3^{2\nu_3}-1)\cdots$$

binäre Substitutionen (17^a). Die Summe aller so gebildeten Anzahlen hat demnach den Werth $(p-1)^2$, was ja auch leicht zu verificiren ist. —

An zweiter Stelle betrachten wir den Fall II), dass $D \equiv 0$ und also

$$\varrho_1 \equiv \frac{a+b'}{2}$$

die einzige, aber doppelt zu rechnende Congruenzwurzel von (19) ist. Es giebt dann eine Function

$$h_1 = m_1 h + n_1 k \equiv a'h + (\varrho_1 - a)k \equiv a'h + \frac{b'-a}{2}k,$$

welche durch (17) in eins ihrer Vielfachen, $\varrho_1 h_1$ umgewandelt wird; ausser den Vielfachen von h_1 giebt es keine solche Function.

Wir suchen ferner, eine zweite Function

$$k_1 = m_2 h + n_2 k$$

zu bestimmen, die durch (17) in $h_1 + \varrho_1 k_1$ übergeführt wird. Dazu muss das System der linearen Congruenzen

$$(18^a) \qquad \begin{aligned} m_2(a-\varrho_1) + n_2 a' &\equiv m_1 \\ m_2 b + n_2(b'-\varrho_1) &\equiv n_1 \end{aligned} \quad (\text{mod. } p)$$

nach m_2, n_2 lösbar sein. Das ist nun in der That der Fall. Denn es ist zwar die Determinante der Coefficienten von m_2, n_2 gleich Null, allein die beiden Systeme, welche sich aus den Constanten bilden lassen,

$$\begin{matrix} a-\varrho_1, & a' \\ b\;\;, & b'-\varrho_1 \end{matrix} \quad \text{und} \quad \begin{matrix} a-\varrho_1, & a'\;\;, & m_1 \\ b\;\;, & b'-\varrho_1, & n_1 \end{matrix}$$

sind, wie die Bestimmung von m_1, n_1 ergiebt, von gleichem Range (§ 479), und daher kann man geeignete m_2 und n_2 angeben, welche die obigen Congruenzen lösen. Da ferner

$$m_1 : n_1 = a' : (\varrho_1 - a) = (\varrho_1 - b') : b$$

und also

$$\begin{aligned} a - \varrho_1 &= \varepsilon n_1, & a' &= -\varepsilon m_1 \\ b' - \varrho_1 &= -\vartheta m_1, & b &= \vartheta n_1 \end{aligned}$$

ist, so wird unter Berücksichtigung von (18^a)

$$m_2(a-\varrho_1)+n_2a'=\varepsilon(m_2n_1-m_1n_2)=m_1,$$
$$m_2b+n_2(b'-\varrho_1)=\vartheta(m_2n_1-m_1n_2)=n_1.$$

Folglich ist $(m_1n_2-m_2n_1)$ nicht congruent 0 mod. p, da m_1 und n_1 nicht gleichzeitig $\equiv 0$ sind, und h, k können durch h_1, k_1 dargestellt werden.

In diesem Falle sind wir zu einer Normalform von der Gestalt

$$(17^b)\qquad u\equiv|h,k\quad \varrho_1h,\ h+\varrho_1k|\quad(\text{mod. }p)$$

gelangt. Hier ist die λ^{te} Potenz dieser Substitution

$$u^\lambda\equiv|h,k\quad \varrho_1^\lambda h,\ \lambda\varrho_1^{\lambda-1}h+\varrho_1^\lambda k|\quad(\text{mod. }p);$$

daraus erkennt man, für welche Werthe von λ die Potenz $u^\lambda=u$ werden wird: Es müssen gleichzeitig die Congruenzen

$$\varrho_1^\lambda\equiv\varrho_1,\quad \lambda\varrho_1^{\lambda-1}\equiv 1\quad(\text{mod. }p)$$

und folglich auch

$$\varrho_1^{\lambda-1}\equiv 1,\quad \lambda\equiv 1\quad(\text{mod. }p)$$

erfüllt sein. Die erste zeigt, dass $\lambda-1$ ein Vielfaches des Exponenten q ist, zu dem ϱ_1 gehört; die zweite, dass λ die Form $\varkappa p+1$ hat. Demgemäss muss $\lambda-1$ d. h. $\varkappa p$ nun auch ein Vielfaches von q sein, damit $\varrho_1^\lambda=\varrho_1$ werde; folglich muss $\varkappa$ selbst ein Vielfaches von q sein; man hat daher $\lambda=\mu(p-1)p+1$ bei jedem ganzzahligen μ. Es wird demnach $u^{(p-1)p+1}\equiv u$ für jedes mögliche u von der Form (17^b), weil q ein Theiler von $p-1$ ist d. h. die Ordnung jeder Substitution zweiter Art ist ein Theiler von $(p-1)p$. —

Endlich an dritter Stelle nehmen wir an III), dass D ein quadratischer Nichtrest für p sei. Am einfachsten können wir diesen Fall durch die Einführung von imaginären Congruenzwurzeln erledigen, wie das zuerst Galois*) gethan hat.

Es sei N irgend einer der $\frac{p-1}{2}$ Nichtreste von p unter den Zahlen $1, 2, \cdots p-1$. Wir definiren j als Wurzel der Congruenz

$$(20)\qquad j^2\equiv N\quad(\text{mod. }p)$$

und wollen mit j rechnen, wie mit einer reellen Zahl; dabei kann überall statt j^2 eingesetzt werden N. Dann lassen sich die Wurzeln von

$$(19)\qquad \varrho^2-\varrho(a+b')+(ab'-a'b)\equiv 0\quad(\text{mod. }p),$$

wenn D ein Nichtrest ist, in die Form

$$\varrho_1=m+nj,\quad \varrho_2=m-nj$$

*) Sur la théorie des nombres. Bullet. des Scienc. math. de Férussac 13 (1830), p. 428; Oeuvres publiées par É. Picard (1897), p. 15.

bringen; denn es ist $D:N$ ein Rest, den man gleich n^2 setzen kann; also dürfen wir $D = n^2 N$ annehmen.

Wir können dann weiter wie im ersten Falle verfahren und als Normalform

$$u \equiv |h, k \quad (m+nj)h, (m-nj)k| \tag{17^c}$$

aufstellen. Zu beachten ist dabei, dass die Indices h, k hier nicht reell sind, sondern in Beziehung auf j als „conjugirt complex" auftreten, d. h. dass sie die Form $(s+tj)$ und $(s-tj)$ haben. Hierbei ist u mit der reellen Substitution

$$\left| \frac{h+k}{2}, \frac{h-k}{2j} \quad \frac{\varrho_1 h + \varrho_2 k}{2}, \frac{\varrho_1 h - \varrho_2 k}{2j} \right|$$

identisch, deren Form aber weniger bequem ist.

Es handelt sich nun noch um die Bestimmung der Ordnung von (17^c). Erheben wir $m+nj$ in die Potenz mit dem Exponenten p, so wird (mod. p)

$$(m+nj)^p \equiv m^p + n^p j^p \equiv m + nj^{p-1}\cdot j \equiv m + N^{\frac{p-1}{2}} n\cdot j;$$

daraus folgt ebenso weiter

$$(m+nj)^{p\cdot p} \equiv m^p + N^{\frac{p(p-1)}{2}} n^p N^{\frac{p-1}{2}} j$$
$$\equiv m + nN^{\frac{p^2-1}{2}}\cdot j \quad (\text{mod.}\, p),$$

und da $\frac{p^2-1}{2}$ ein ganzes Vielfaches von $(p-1)$ ist,

$$\equiv m + nj,$$

so dass also jede unserer neuen complexen Zahlen in die Potenz (p^2-1) erhoben gleich der Einheit wird. Es kann deshalb die Ordnung von (17^c) nur ein Theiler dieses Exponenten (p^2-1) sein.

In der Congruenz

$$(m+nj)^{p\cdot p} \equiv (m+nj) \quad (\text{mod.}\, p)$$

ist der Fermat'sche Satz für unser Zahlengebiet enthalten.

Verstehen wir unter $\varphi(u)$ die zahlentheoretische Function, welche angiebt, wie viele ganze, positive Zahlen kleiner als u und theilerfremd zu u sind, so folgt genau durch die in der Zahlentheorie üblichen Schlüsse, dass, wenn man unter f einen Theiler von (p^2-1) versteht, zu dem Exponenten f gerade $\varphi(f)$ Zahlen $(m+nj)$ gehören, d. h. dass $\varphi(f)$ Zahlen vorhanden sind, deren f^{te} Potenz der Einheit congruent wird, während niedere Potenzen dieser Zahlen nicht $\equiv 1$ werden.

Erweitert man auf unser Gebiet den Begriff der primitiven Wurzeln, so ergiebt sich wieder, dass gerade $\varphi(p^2-1)$ Zahlen $(m_0+n_0 j)$ primitive Wurzeln sind, und dass jede Zahl $(m+nj)$ einer Potenz irgend einer solchen primitiven Wurzel $(m_0+n_0 j)$ congruent wird.

§ 538. Mit den Untersuchungen des vorigen Paragraphen hängt eine andere Frage zusammen, die wir hier erledigen wollen. Betrachtet man in der homogenen linearen Substitution mit reellen Coefficienten

$$v = |h, k \quad ah+bk, a'h+b'k|$$

die wirklichen Werthe der Indices, statt wie bisher ihre Reste modulo p, so kann man auch hier fragen, unter welchen Bedingungen eine Potenz von v gleich der Einheit wird; im Allgemeinen nämlich werden sämmtliche Potenzen der Substitution v von einander verschieden sein.

Damit v überhaupt eine Substitution darstelle, muss $(ab'-a'b) \neq 0$ sein.

Wir können nun genau wie im vorigen Paragraphen den Versuch machen, eine Function $(mh+nk)$ zu bestimmen, welche durch v in ein Vielfaches $\varrho(mh+nk)$ verwandelt wird. Damit dies möglich sei, müssen m, n, ϱ den Gleichungen

$$\begin{aligned} m(a-\varrho)+na' &= 0 \\ mb+n(b'-\varrho) &= 0 \end{aligned} \tag{18*}$$

Genüge leisten. Also muss ϱ eine Wurzel der Gleichung

$$\varrho^2-\varrho(a+b')+(ab'-a'b) = 0 \tag{19*}$$

sein.

Hierbei unterscheiden wir wie oben drei Fälle, je nachdem nämlich in dem Ausdrucke für die Wurzeln

$$\varrho = \frac{a+b'}{2} \pm \sqrt{\left(\frac{a+b'}{2}\right)^2+(a'b-ab')}$$

der Radicand positiv, Null, oder negativ ist.

Im ersten Falle seien ϱ_1, ϱ_2 die beiden Wurzeln von (19*) und

$$w = |h, k \quad \varrho_1 h, \varrho_2 k|$$

die Normalform. Damit jetzt $w^\lambda = 1$ werde, muss $\varrho_1^\lambda = 1$, $\varrho_2^\lambda = 1$ werden; es müssen also ϱ_1 und ϱ_2 zwei reelle λ^{te} Einheitswurzeln sein, d. h. sie müssen die Werthe $+1$, -1 annehmen. Das ist nur möglich bei

$$a+b'=0, \quad a'b-ab'=+1,$$

und λ nimmt den Werth 2 an. In der That findet man für jede solche Form

$$w = \left| h, k \quad ah + bk, \frac{1-a^2}{b} h - ak \right|$$

die zweite Potenz gleich der Einheit. —

Im zweiten Falle kommen wir wie oben zu einer Normalform

$$w = | h, k \quad \varrho_1 h, h + \varrho_1 k |,$$

für welche

$$w^\lambda = | h, k \quad \varrho_1^\lambda h, \lambda \varrho_1^{\lambda-1} h + \varrho_1^\lambda k |$$

wird. Damit $w^\lambda = w$ wird, muss ϱ_1 eine $(\lambda - 1)^{\text{te}}$ Einheitswurzel und $\lambda = 1$ sein. Also kann für $\lambda > 1$ nie $w^\lambda = w$ werden. —

Im dritten Falle wird die Normalform äusserlich gleich der im ersten Falle

$$w = | h, k \quad \varrho_1 h, \varrho_2 k |;$$

aber hier haben ϱ_1 und ϱ_2 die conjugirt complexen Werthe

$$\frac{a+b'}{2} + i\sqrt{-\left(\frac{a+b'}{2}\right)^2 + (ab' - a'b)},$$

$$\frac{a+b'}{2} - i\sqrt{-\left(\frac{a+b'}{2}\right)^2 + (ab' - a'b)}.$$

Damit $w^\lambda = 1$ wird, müssen beide Werthe conjugirt complexe λ^{te} Einheitswurzeln sein,

$$\frac{a+b'}{2} \pm i\sqrt{-\left(\frac{a+b'}{2}\right)^2 + (ab' - a'b)} = \cos\frac{2\varkappa\pi}{\lambda} \pm i \sin\frac{2\varkappa\pi}{\lambda},$$

d. h. also

$$a + b' = 2\cos\frac{2\varkappa\pi}{\lambda}; \quad ab' - a'b = 1. \tag{21}$$

In der That findet man auch, wenn die Bedingungen (21) erfüllt sind, für ϱ_1, ϱ_2 die Werthe $\cos\frac{2\varkappa\pi}{\lambda} + i\sin\frac{2\varkappa\pi}{\lambda}$ und $\cos\frac{2\varkappa\pi}{\lambda} - i\sin\frac{2\varkappa\pi}{\lambda}$, und also $w^\lambda = 1$.

Man erkennt sofort den inneren Zusammenhang zwischen dieser Untersuchung und der gelegentlich der Frage nach den Iterationen einer gebrochenen linearen Function angestellten (Vorles. 24; Bd. I).

Vierundfünfzigste Vorlesung.

Functionengattungen.

§ 539. Durch die Untersuchungen der letzten Vorlesungen sind wir zu der Bildung eines wichtigen Begriffes, dem der Gattungen von Functionen geführt worden, auf welchen wir nunmehr genauer eingehen müssen.

Es seien n von einander unabhängige, unbestimmte Grössen z_1, $z_2, \cdots z_n$ gegeben. Wir haben symmetrische Functionen dieser Grössen gebildet und gesehen, dass diese für alle $n!$ Substitutionen der z ungeändert bleiben; diese $n!$ Substitutionen bilden die symmetrische Gruppe; jede Function, die für alle diese Substitutionen ihre Form nicht ändert, ist eine symmetrische Function. Sämmtliche symmetrische Functionen wollen wir zu einer Gattung rechnen, der symmetrischen Gattung.

Wir haben dann weiter (§ 519) eine alternirende Function

$$\sqrt{D} = \prod_{\lambda,\mu}(z_\lambda - z_\mu) \qquad (\lambda = 1, 2, \cdots n-1;\ \mu = \lambda+1, \cdots n)$$

gebildet und gesehen, dass diese für alle geraden Substitutionen ihre Form beibehielt; diese Substitutionen bildeten die alternirende Gruppe; der Inbegriff aller alternirenden und allgemeiner aller zweiwerthigen Functionen bildet die alternirende Gattung.

In ähnlicher Weise haben wir cyklische Functionen und cyklische Gruppen u. s. f. zusammengestellt; wir fassen die Functionen jedesmal zu einer Gattung zusammen.

Wir wollen nun allgemeiner eine beliebige, ganze, rationale Function von n unabhängigen Elementen $z_1, z_2, \cdots z_n$

$$\varphi(z_1, z_2, \cdots z_n) = \varphi_1 \tag{1}$$

bilden und alle die Substitutionen ins Auge fassen, deren Anwendung auf φ die Form und damit den Werth dieser Function nicht ändert. Sind s_λ und s_μ zwei solche Substitutionen, so wird, wenn wir das Resultat ihrer Anwendung auf φ_1 mit φ_{s_λ} und φ_{s_μ} bezeichnen,

$$(\varphi_{s_\mu})_{s_\lambda} = \varphi_{s_\lambda} = \varphi_1; \quad (\varphi_{s_\lambda})_{s_\mu} = \varphi_{s_\mu} = \varphi_1,$$

d. h. die Folgen $s_\mu s_\lambda$ und $s_\lambda s_\mu$ gehören auch zu den Substitutionen, die (1) nicht ändern; ihre Gesammtheit bildet eine Gruppe G. Diese Gruppe ordnen wir der Function φ zu; wir sagen: die Function φ gehört zu der Gruppe G und umgekehrt, die Gruppe G gehört zu der Function φ. Besteht G aus den r Substitutionen, unter denen natürlich die Einheitssubstitution vorkommt,

$$s_1 = 1,\ s_2,\ s_3,\ \cdots\ s_r, \tag{2}$$

so bilden die r Substitutionen, bei denen s_α ein beliebiges Element aus (2) selbst bezeichnen soll,

$$s_1 s_\alpha,\ s_2 s_\alpha,\ s_3 s_\alpha,\ \cdots\ s_r s_\alpha \qquad (\alpha = 1, 2, \cdots r) \tag{3}$$

gleichfalls die Gruppe G; denn diese Producte kommen sämmtlich

in G vor und sind alle unter einander verschieden. Das Gleiche gilt von der Reihe

$$(4)\qquad s_\alpha s_1,\ s_\alpha s_2,\ s_\alpha s_3,\ \cdots s_\alpha s_r \qquad (\alpha = 1, 2, \cdots r).$$

Insbesondere erkennt man, da 1 auch in (3) und in (4) vorkommen muss, dass mit jedem s_α auch s_α^{-1} in (2) auftritt.

Aus dem Vorhergehenden ist es klar, dass zu jeder Function eine Substitutionengruppe gehört. Es fragt sich, ob umgekehrt zu jeder irgendwie definirten Gruppe eine Function gefunden werden kann. Durch die Behandlung dieses allgemeinen Problems erledigen wir eine Reihe von Fragen, die früher jedesmal in Specialfällen behandelt werden mussten. Es wird sich zeigen, dass zu jeder Gruppe unendlich viele, miteinander durch wichtige gemeinsame Eigenschaften verknüpfte Functionen existiren; diese schliessen wir dann in eine Functionengattung zusammen, welche durch die Gruppe als ihre Invariante eindeutig bestimmt ist. Solche Gattungen (symmetrische, alternirende, cyklische u. s. f.) haben wir schon mehrfach benutzt.

Wir wollen zunächst die einfachste Gruppe unseren Betrachtungen zu Grunde legen, nämlich die aus der identischen Substitution 1 allein bestehende Gruppe der Ordnung 1. Eine zugehörige Function $\varphi = \varphi_1$ muss daher bei jeder der $n!$ vorhandenen Substitutionen einen anderen Werth annehmen. Daraus folgt, dass φ unter dem Einflusse verschiedener Substitutionen auch stets verschiedene Werthe erhält. Denn aus der Gleichung

$$\varphi_{s_\alpha} = \varphi_{s_\beta} \quad \text{würde folgen} \quad \varphi_{s_\alpha s_\beta^{-1}} = \varphi_{s_\beta s_\beta^{-1}} = \varphi_1,$$

d. h. φ bliebe für $s_\alpha s_\beta^{-1}$ ungeändert, und es müsste infolge unserer Voraussetzung $s_\alpha s_\beta^{-1} = 1$, d. h. $s_\alpha = s_\beta$ sein. Es hat demnach φ_1 so viele Werthe als es Substitutionen giebt nämlich $n!$; φ ist eine $n!$-werthige Function; die Functionen dieser Gattung nehmen daher soviele Werthe an, als überhaupt möglich sind.

Derartige Functionen lassen sich in mannigfacher Art herstellen. Bedeuten $u_0, u_1, \cdots u_n$ unbestimmte Parameter, so genügt z. B. jedes lineare Aggregat

$$(5)\qquad \varphi_1 = u_0 + u_1 z_1 + u_2 z_2 + \cdots + u_n z_n$$

der Forderung; denn wenn s_α die Umänderung der Function φ_1 in

$$\varphi_{s_\alpha} = u_0 + u_1 z_{\alpha_1} + u_2 z_{\alpha_2} + \cdots + u_n z_{\alpha_n}$$

hervorruft, wobei die $z_{\alpha_1}, \cdots z_{\alpha_n}$ nur eine Umstellung der $z_1, \cdots z_n$ bedeuten, dann kann wegen der Unbestimmtheit der u nur dann $\varphi_1 = \varphi_{s_\alpha}$ sein, wenn jedes $z_{\alpha_\varkappa} = z_\varkappa$ wäre, d. h. wenn s_α alle Elemente z ungeändert liesse.

In ähnlicher Weise folgt, dass auch der Ausdruck

$$(5^a) \qquad \psi_1 = u_0 z_1^{u_1} z_2^{u_2} \cdots z_n^{u_n}$$

zur Gruppe 1 gehört, wenn die u wieder unbestimmte Grössen bedeuten, die sogar positiv und ganzzahlig sein dürfen.

Wir haben bisher vorausgesetzt, dass die Grössen $z_1, z_2, \cdots z_n$ unbestimmte Grössen seien. Wir wollen jetzt annehmen, die z seien fest gegebene Grössen, zwischen denen beliebige numerische Beziehungen statthaben können. Es ist nun möglich, in diesem Falle eine $n!$-werthige Function φ_1 so zu bilden, dass auch bei der Substitution dieser fest gegebenen Grössen $\zeta_1, \zeta_2, \cdots \zeta_n$ statt $z_1, z_2, \cdots z_n$, die $n!$-Werthe φ unter einander numerisch verschieden bleiben, so lange nicht zwei oder mehrere Werthe $\zeta_1, \zeta_2, \cdots \zeta_n$ einander gleich werden. In diesem letzten Falle ist eine solche Function $\varphi(z_1, z_2, \cdots z_n)$ natürlich nicht vorhanden; denn wäre z. B. $\zeta_1 = \zeta_2$, dann würde $\varphi(\zeta_1, \zeta_2, \zeta_3, \cdots \zeta_n) = \varphi(\zeta_2, \zeta_1, \zeta_3, \cdots \zeta_n)$ werden, wie φ auch gewählt wird. Wir schliessen daher den Fall aus, dass numerische Relationen $\zeta_\alpha = \zeta_\beta$ unter den ζ vorkommen.

Wenn nun alle ζ unter einander verschieden sind, dann sei M das Maximum und m das Minimum der absoluten Beträge der Differenzen zweier ζ,

$$|\zeta_1 - \zeta_2|, \quad |\zeta_1 - \zeta_3|, \quad |\zeta_2 - \zeta_3|, \quad \cdots \quad |\zeta_{n-1} - \zeta_n|;$$

wir wählen jetzt eine Constante u_1 beliebig und die weiteren Constanten $u_2, u_3, \cdots$ nur den Bedingungen

$$m \cdot |u_2| > M \cdot |u_1|; \quad m \cdot |u_3| > M \cdot (|u_1| + |u_2|), \cdots$$
$$m \cdot |u_n| > M \cdot (|u_1| + \cdots + |u_{n-1}|)$$

unterworfen. Aus einer Gleichung zwischen den beiden linearen Aggregaten

$$u_0 + u_1\zeta_{i_1} + u_2\zeta_{i_2} + \cdots + u_n\zeta_{i_n} = u_0 + u_1\zeta_{k_1} + u_2\zeta_{k_2} + \cdots + u_n\zeta_{k_n}$$

würde dann folgen, wenn ζ_{i_n} von ζ_{k_n} verschieden wäre,

$$u_n(\zeta_{i_n} - \zeta_{k_n}) = u_{n-1}(\zeta_{k_{n-1}} - \zeta_{i_{n-1}}) + \cdots + u_1(\zeta_{k_1} - \zeta_{i_1}),$$
$$|u_n| \cdot |\zeta_{i_n} - \zeta_{k_n}| < M \cdot (|u_1| + |u_2| + \cdots + |u_{n-1}|).$$

Nach unseren Festsetzungen ist aber bei verschiedenen ζ_{i_n}, ζ_{k_n} in Widerspruch zu dieser Ungleichung stets

$$|u_n| \cdot |\zeta_{i_n} - \zeta_{k_n}| > M(|u_1| + |u_2| + \cdots + |u_{n-1}|).$$

Demgemäss muss $\zeta_{i_n} = \zeta_{k_n}$ sein. Aus der resultirenden Gleichung

$$u_0 + u_1\zeta_{i_1} + \cdots + u_{n-1}\zeta_{i_{n-1}} = u_0 + u_1\zeta_{k_1} + \cdots + u_{n-1}\zeta_{k_{n-1}}$$

würde dann ebenso $\zeta_{i_{n-1}} = \zeta_{k_{n-1}}$ folgen, u. s. f., bis auf $\zeta_{i_1} = \zeta_{k_1}$; d. h. die beiden einander numerisch gleichen Ausdrücke würden identisch, und $s_i = s_k$.

Zu diesem Satze können wir noch hinzufügen, dass u_0 auf unendlich viele Arten so gewählt werden kann, dass auch die absoluten Werthe der $\varphi_1(\zeta_1, \cdots \zeta_n)$, $\varphi_{s_i}(\zeta_1, \cdots \zeta_n), \cdots$ sämmtlich unter einander verschieden ausfallen. In der That, setzt man etwa bei allgemeinen complexen Werthen der u und der ζ

$$u_1 \zeta_{\alpha_1} + \cdots + u_n \zeta_{\alpha_{n_1}} = \sigma_\alpha + \tau_\alpha \cdot i,$$
$$u_0 = p + q \cdot i,$$

dann kommt es nur darauf an, die beiden Constanten p und q so zu wählen, dass alle Ausdrücke

$$(p + \sigma_\alpha)^2 + (q + \tau_\alpha)^2 = p^2 + q^2 + 2\sigma_\alpha p + 2\tau_\alpha q + \sigma_\alpha^2 + \tau_\alpha^2$$
$$(\alpha = 1, 2, \cdots n!)$$

von einander verschieden ausfallen. Das ist, wenn man z. B. $p = q^3$ und q hinreichend gross annimmt, auf reellem Gebiete stets zu erreichen, wie man leicht sieht.

Da wir dieselben Schlüsse auch auf $\log \zeta_1$, $\log \zeta_2, \cdots \log \zeta_n$ anwenden können, so folgt, dass sich auch in (5^a) die Constanten u so wählen lassen, dass $\psi_1(\zeta_1, \cdots \zeta_n)$ nach wie vor $n!$ von einander verschiedene Werthe annimmt, falls eben nur die $\zeta_1, \zeta_2, \cdots \zeta_m$ von einander verschiedene Werthe besitzen.

Die hier zu Grunde gelegte Gruppe mit der einzigen Substitution 1 ist gewissermassen der andere Pol zur symmetrischen, welche alle Substitutionen umfasst. Wir wollen sie die Galois'sche Gruppe und die zu ihr gehörigen Functionen, deren Existenz wir eben hergeleitet haben, Galois'sche Functionen nennen. Diese wollen wir zu der Galois'schen Gattung vereinigen.

Mit Hülfe solcher $n!$-werthigen Galois'schen Functionen kann man leicht zu jeder anderen Gruppe G zugehörige Functionen construiren. Besteht G aus den Substitutionen (2), so bilden wir aus einer $n!$-werthigen Function $\varphi = \varphi_1$ die r Werthe, welche durch jene Substitutionen $s_1, s_2, \cdots s_r$ aus φ hervorgehen

$$\varphi_1 = \varphi, \ \varphi_{s_2}, \ \varphi_{s_3}, \ \cdots \ \varphi_{s_r}, \tag{6}$$

und aus ihnen setzen wir eine symmetrische Function, etwa die Potenzsumme zusammen

$$\Phi = \varphi_1^\varkappa + \varphi_{s_2}^\varkappa + \varphi_{s_3}^\varkappa + \cdots + \varphi_{s_r}^\varkappa,$$

in welcher $\varkappa$ noch unbestimmt bleiben soll. Φ bleibt für jedes s_α von G ungeändert, da ja wegen der bei (3) gemachten Bemerkung der Werth

$$\Phi_{s_\alpha} = \varphi_{s_\alpha}^\varkappa + \varphi_{s_2 s_\alpha}^\varkappa + \cdots + \varphi_{s_r s_\alpha}^\varkappa = \Phi \qquad (\alpha = 1, 2, \cdots r)$$

wird. Es ist aber, damit Φ zu G gehöre, umgekehrt auch nothwendig, dass Φ_σ nur für Substitutionen σ der vorgelegten Gruppe G gleich Φ werde. Um dies zu erreichen, treffen wir die folgenden Vorkehrungen. Es seien die $\varphi_1, \varphi_2, \varphi_3, \cdots$ nach absteigenden Werthen ihrer absoluten Beträge geordnet, durch $\chi_1, \chi_2, \chi_3, \cdots$ dargestellt. Dann lässt sich der Exponent $\varkappa$ so wählen, dass die Ungleichungen

$$|\chi_1^\varkappa| > |\chi_2^\varkappa| + |\chi_3^\varkappa| + \cdots; \quad |\chi_2^\varkappa| > |\chi_3^\varkappa| + |\chi_4^\varkappa| + \cdots;$$
$$|\chi_{r-1}^\varkappa| > |\chi_r^\varkappa|$$

gelten. Ist dies geschehen, dann kann eine Gleichung mit willkürlichen Indices $\alpha, \beta, \cdots; \varepsilon, \zeta, \cdots$

$$\chi_\alpha^\varkappa + \chi_\beta^\varkappa + \cdots = \chi_\varepsilon^\varkappa + \chi_\zeta^\varkappa + \cdots$$

nur dann stattfinden, wenn alle Glieder der einen Seite auch auf der anderen Seite vorkommen. Wenden wir dies auf $\Phi_\sigma = \Phi_1$ an, dann folgt bei dieser Wahl des Exponenten, dass σ die Werthe $\varphi_1, \varphi_{s_2}, \cdots \varphi_{s_r}$ unter einander umwandelt und also zu G gehört; denn φ ist ja so eingerichtet, dass es $n!$ Werthe hat, und dass jedem Werthe eine Substitution entspricht, deren Anwendung auf φ gerade diesen Werth hervorruft. —

Für die Rechnung stellt es sich bequemer, eine Function

$$\Psi = \psi_1 + \psi_{s_2} + \psi_{s_3} + \cdots + \psi_{s_r}$$

mit Hülfe von (5ᵃ) zu bilden. Auch hier kann man auf unendlich viele Arten so vorgehen, dass Ψ für alle und nur für die Substitutionen der Gruppe G ungeändert bleibt.

Eine andere Methode, Functionen zu construiren, die zu G gehören, ist die folgende. Nachdem wir eine $n!$-werthige lineare Function

$$(5) \qquad \varphi_1 = u_0 + u_1 z_1 + \cdots + u_n z_n$$

hergestellt haben, bilden wir mit einer Unbestimmten u das Product

$$\prod_\lambda (u - \varphi_{s_\lambda}) \qquad (\lambda = 1, 2, \cdots r).$$

Dies bleibt für alle Substitutionen $s_1, s_2, \cdots s_r$ von G ungeändert. Wenn umgekehrt für irgend eine Substitution σ

$$\prod_\lambda (u - \varphi_{s_\lambda \sigma}) = \prod_\lambda (u - \varphi_{s_\lambda})$$

ist, dann folgt wegen der Unbestimmtheit des u, dass die linearen Factoren beider Seiten mit einander übereinstimmen müssen. Um dies einzusehen reicht es aus, u gleich einem $\varphi_{s_\lambda \sigma}$ zu setzen. Insbesondere wird $(u - \varphi_\sigma)$ unter den $(u - \varphi_{s_\lambda})$ vorkommen. φ_σ muss daher gleich einem φ_{s_λ} sein. Weil nun φ als $n!$-werthige Function angenommen wurde, so ist dies nur möglich, wenn $\sigma = s_\lambda$ ist, d. h. wenn σ selbst der Gruppe G angehört.

Von dieser Construction werden wir in der siebenundfünfzigsten Vorlesung wichtige Vortheile ziehen können.

Endlich ist noch zu erwähnen, dass die gemeinsamen Substitutionen zweier Gruppen selbst wieder eine Gruppe bilden. Denn sind z. B. die beiden Gruppen G und G_1 gegeben, und gehört zur ersten $\varphi(z_1, \cdots)$ und zur zweiten $\psi(z_1, \cdots)$, dann wird die Function

$$\varphi(z_1, \cdots) + u\psi(z_1, \cdots),$$

in der u eine Unbestimmte bedeutet, nur für eine Substitution ungeändert bleiben, welche sowohl φ als ψ ungeändert lässt, also zu G und zu G_1 gehört. Umgekehrt lässt jede zu G und zu G_1 gehörige Substitution $\varphi + u\psi$ ungeändert. Alle gemeinsamen Substitutionen bilden folglich die zu $\varphi + u\psi$ gehörige Gruppe.

Für die folgenden Betrachtungen wollen wir nun wieder die z als unbestimmte Grössen voraussetzen, so lange das Gegentheil nicht ausdrücklich bemerkt wird.

§ 540. Durch die eben besprochene Methode, Functionen herzustellen, die einer gewissen Gruppe G von Substitutionen angehören, haben wir die Existenz der zugehörigen Functionengattung nachgewiesen. Ist also eine Gruppe G gegeben, so kann man beliebig viele Functionen construiren, die für die Substitutionen von G und nur für diese ungeändert bleiben (auch wenn für die z feste, von einander verschiedene, sonst aber ganz willkürliche Werthe gegeben sind). Und wenn umgekehrt eine Function der n Grössen z gegeben ist, dann kann man durch Untersuchung des Einflusses, welchen jede der $n!$ Substitutionen auf die Function ausübt, die Gruppe bestimmen, die zu dieser Function gehört.

Es ist leicht einzusehen, dass es nur eine endliche Anzahl von Gattungen giebt. Dazu reicht es aus, zu bedenken, dass die $n!$ Substitutionen nur eine endliche Anzahl von Gruppen zulassen.

Die Zugehörigkeit zu derselben Gruppe von Substitutionen entscheidet darüber, ob Functionen derselben Gattung angehören. Es giebt aber weiter noch andere Eigenthümlichkeiten algebraischer Natur,

durch welche Functionen derselben Gattung mit einander verknüpft sind. Zu diesen wenden wir uns jetzt.

I) Ist G mit den Substitutionen (2) die vorgelegte Gruppe, und bezeichnen wir $\frac{n!}{r} = \varrho$, so ist jede zu G gehörige Function φ_1 die Wurzel einer Gleichung ϱ^{ten} Grades, deren Coefficienten in den z symmetrisch sind.

Bei symmetrischen Functionen ist $r = n!$ und $\varrho = 1$, so dass hier der Satz selbstverständlich wird.

Ist φ_1 nicht symmetrisch, so giebt es ausser den zu G gehörigen Substitutionen

$$(2) \qquad s_1 = 1, \; s_2, \; s_3, \cdots s_r$$

noch eine neue σ_2, welche φ_1 in einen anderen Werth $\varphi_{\sigma_2} = \varphi_2$ umwandelt. Die Substitutionen, welche aus rechtsseitiger Multiplication von (2) mit σ_2 entstehen nämlich

$$(2^a) \qquad \sigma_2, \; s_2\sigma_2, \; s_3\sigma_2, \cdots s_r\sigma_2,$$

sind (§ 508, E) sämmtlich unter einander und von (2) verschieden; sie rufen sämmtlich den gleichen Werth φ_2 hervor, da ja

$$\varphi_{s_\varkappa\sigma_2} = (\varphi_{s_\varkappa})_{\sigma_2} = (\varphi_1)_{\sigma_2} = \varphi_{\sigma_2} = \varphi_2$$

ist. Und sie sind auch die einzigen dieser Eigenschaft. Denn aus $\varphi_\tau = \varphi_{\sigma_2}$ folgt $\varphi_{\tau\sigma_2^{-1}} = \varphi_1$; also gehört $\tau\sigma_2^{-1}$ zu (2), d. h. es wird sein

$$\tau\sigma_2^{-1} = s_\varkappa, \quad \tau = s_\varkappa\sigma_2.$$

Giebt es ausser (2) und (2^a) andere Substitutionen der n Elemente z, ist also $n! > 2r$, so sei σ_3 eine solche Substitution; sie ruft einen von φ_1 und φ_2 verschiedenen Werth $\varphi_{\sigma_3} = \varphi_3$ hervor. Wir betrachten nun die Substitutionen, die ähnlich wie (2^a) gebildet sind,

$$(2^b) \qquad \sigma_3, \; s_2\sigma_3, \; s_3\sigma_3, \cdots s_r\sigma_3$$

und können von ihnen die entsprechenden Eigenschaften wie von (2^a) nachweisen: sie sind unter sich und von (2) und (2^a) verschieden; sie wandeln sämmtlich φ in φ_3 um; und nur sie haben diese Wirkung.

In dieser Art können wir fortgehen bis zu einem Functionenwerthe φ_ϱ und einer Substitutionenreihe, mit welcher das Schema (2), (2^a), (2^b) $\cdots$ abschliesst,

$$(2^c) \qquad \sigma_\varrho, \; s_2\sigma_\varrho, \; s_3\sigma_\varrho, \cdots s_r\sigma_\varrho.$$

Die Reihen (2), (2^a), (2^b), $\cdots$ (2^c) enthalten jetzt sämmtliche $n!$ Substitutionen, sodass also $r \cdot \varrho = n!$ ist. φ_1 ist eine ϱ-werthige Function; die Anzahl der Werthe einer Function φ_1 ist ein Theiler von $n!$.

Die Anordnung der $n!$ Substitutionen in die Reihen (2), (2ᵃ), $\cdots$ ist von der Wahl der $\sigma_2, \sigma_3, \cdots \sigma_\varrho$ unabhängig. Denn nimmt man z. B. statt σ_α ein $s_\varkappa \sigma_\alpha$, welches der gleichen Zeile wie σ_α angehört, dann wird der Complex

$$(s_\varkappa \sigma_\alpha), \quad s_2(s_\varkappa \sigma_\alpha), \quad s_3(s_\varkappa \sigma_\alpha), \cdots$$

bis auf die Reihenfolge mit dem durch σ_α hervorgerufenen

$$\sigma_\alpha, \quad s_2 \sigma_\alpha, \quad s_3 \sigma_\alpha, \cdots$$

übereinstimmen, da der Complex

$$s_\varkappa, \quad s_2 s_\varkappa, \quad s_3 s_\varkappa, \cdots \quad \text{mit} \quad 1, \quad s_2, \quad s_3, \cdots$$

übereinstimmt (vgl. Formel (3) § 539).

Ferner ist diese Anordnung von der Wahl der zur gegebenen Gruppe gehörigen Function φ unabhängig. Denn gehört auch $\chi(z_1, \cdots z_n) = \chi_1$ zu (2), dann wird σ_2 die Function χ in ein χ_2 überführen, wobei $\chi_2 \neq \chi_1$ ist. Alle (2ᵃ) thun dasselbe, und auch nur sie; u. s. f. Hieraus folgt, dass die Werthe φ_1 und χ_1, ebenso φ_2 und $\chi_2, \cdots$ sich einander derart zuordnen, dass jede Substitution der symmetrischen Gruppe gleichzeitig φ_α in φ_β und χ_α in χ_β umändert.

Nach § 105, Bd. I ist jede symmetrische Function

$$S(\varphi_1, \varphi_2, \cdots \varphi_\varrho)$$

aller Werthe von φ eine symmetrische Function der $z_1, z_2, \cdots z_n$, und wenn daher t eine unbestimmte Grösse bedeutet, dann wird der Ausdruck

$$(7) \quad (t-\varphi_1)(t-\varphi_2)\cdots(t-\varphi_\varrho) \equiv t^\varrho - C_1 t^{\varrho-1} + C_2 t^{\varrho-2} - \cdots \pm C_\varrho$$

eine ganze Function von t, deren Coefficienten symmetrische Functionen der z sind. Die Gleichung

$$(7^a) \qquad t^\varrho - C_1 t^{\varrho-1} + C_2 t^{\varrho-2} - \cdots \pm C_\varrho \equiv \Phi(t) = 0$$

hat daher die ϱ Werthe $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ zu Wurzeln. Dies ist die Gleichung ϱ^{ten} Grades, von welcher in dem Theorem zu Anfang dieses Paragraphen die Rede war. In § 573 werden wir beweisen, dass (7) im Rationalitätsbereiche der symmetrischen Functionen irreductibel ist.

Die verschiedenen Werthe der ϱ-werthigen Function φ nennen wir einander conjuge Werthe. —

II) Gehören φ und χ derselben Gattung an, dann ist jede dieser Functionen rational durch die andere ausdrückbar mit Coefficienten, die in den z symmetrisch sind, und umgekehrt. In der That gehört die rationale gebrochene Function

$$\frac{\chi_1(z_1, \cdots z_n)}{t - \varphi_1(z_1, \cdots z_n)} = \frac{\chi_1}{t - \varphi_1}$$

gleichfalls zu der Gattung von φ_1 und χ_1, und sie nimmt für $\sigma_1 = 1$, $\sigma_2, \sigma_3, \cdots \sigma_\varrho$ die Werthe

$$\frac{\chi_1}{t-\varphi_1}, \quad \frac{\chi_2}{t-\varphi_2}, \quad \cdots \quad \frac{\chi_\varrho}{t-\varphi_\varrho}$$

an. Daher wird die rationale ganze Function von t, welche unter Benutzung von (7ª) gebildet wird,

$$\left(\frac{\chi_1}{t-\varphi_1} + \frac{\chi_2}{t-\varphi_2} + \cdots + \frac{\chi_\varrho}{t-\varphi_\varrho}\right)\Phi(t) = \Psi(t)$$

zugleich eine ganze symmetrische Function der $z_1, z_2, \cdots z_n$. Aus dieser Gleichung folgt dann für $t = \varphi_1$, wie schon häufig früher gezeigt wurde,

$$\chi_1(z_1, z_2, \cdots z_n) = \frac{\Psi(\varphi_1(z_1, \cdots z_n))}{\Phi'(\varphi_1(z_1, \cdots z_n))}; \tag{8}$$

$$\Phi'(\varphi(z_1, \cdots z_n)) = (\varphi_1 - \varphi_2)(\varphi_1 - \varphi_3) \cdots (\varphi_1 - \varphi_\varrho). \tag{9}$$

Man kann die Form (8) so umgestalten, dass der Nenner frei von φ_1 und in den z symmetrisch wird; dafür tritt dann eine Beziehung

$$\chi_1(z_1, \cdots z_n) = \frac{\Omega(\varphi_1(z_1, \cdots z_n))}{\varDelta_\varphi}, \tag{8ª}$$

$$\varDelta_\varphi = \prod (\varphi_\lambda - \varphi_\mu)^2 \quad (\lambda = 1, 2, \cdots \varrho - 1;\ \mu = \lambda + 1, \cdots \varrho) \tag{9ª}$$

auf, d. h. es erscheint die Discriminante von (7) als Nenner des Ausdrucks (8ª). Da $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ von einander verschieden sind, so kann (8) oder (8ª) nicht illusorisch werden.

Hierdurch ist der erste Theil des Satzes bewiesen. Besteht ferner ausser (8) noch umgekehrt eine Gleichung, der gemäss φ_1 durch χ_1 ausgedrückt wird,

$$\varphi_1(z_1, \cdots z_n) \frac{A(\chi_1(z_1, \cdots z_n))}{M'(\chi_1(z_1, \cdots z_n))}, \tag{8*}$$

so folgt aus (8), dass χ_1 für alle Substitutionen ungeändert bleibt, welche φ_1 nicht ändern, und aus (8*), dass φ_1 für alle Substitutionen ungeändert bleibt, die χ_1 nicht ändern. Folglich gehören φ_1 und χ_1 zur selben Gattung.

Der obige Lehrsatz giebt also auch eine rein arithmetische Definition der Functionengattungen: *Alle Functionen, die sich gegenseitig rational durch einander ausdrücken lassen mit Coefficienten, welche in den z symmetrisch sind, bilden eine Gattung.* Aus (8ª) und (7) geht hervor, dass diese Darstellung in der Form einer ganzen Function gegeben werden kann, deren Coefficienten gebrochene symmetrische Functionen mit dem Nenner $\varDelta_\varphi$ sind;

die ganze Function braucht dabei nur bis zum Grade $(\varrho - 1)$ aufzusteigen, da höhere Potenzen von φ sich mit Hülfe von (7) entfernen lassen.

Der abgeleitete wichtige, durch (8) oder (8^a) ausgedrückte Satz stammt von Lagrange*). Er ist unter Wahrung des obigen Beweisganges einer weiteren Ausdehnung fähig, zu der wir zunächst übergehen.

III) Wenn $\chi(z_1, \cdots z_n)$ eine Function bedeutet, die bei der Anwendung von G ungeändert bleibt, dann braucht sie nicht nothwendig zu der durch G charakterisirten Gattung zu gehören; denn es ist möglich, dass sie noch für andere Substitutionen ungeändert bleibt. In diesem Falle sagen wir, χ gehöre einer Gattung an, die unter der Gattung G steht, oder kürzer: χ selbst steht unter der Gattung G (vgl. § 521). Es sei dies die durch G_1 charakterisirte Gattung, deren Ordnung wir durch r_1 bezeichnen wollen. Dann gehört jede Substitution von G zu G_1, d. h. G ist eine Subgruppe oder ein Theiler von G_1, und G ist in G_1 enthalten, wenn die Gattung G_1 unter der Gattung G steht. So steht jede Gattung unter der Galois'schen (§ 539); und umgekehrt steht die symmetrische Gattung unter jeder anderen.

Ist nun σ_2 eine der zur G_1 gehörigen Substitutionen, die nicht in G vorkommen, dann wird σ_2 die Function χ_1 ungeändert lassen, dagegen φ_1 in ein φ_2 umwandeln. Man erkennt nun genau wie bei den obigen Schlüssen, dass alle Substitutionen (2^a) gleichfalls φ_1 in φ_2 umwandeln, und dass dies die einzigen dieser Eigenschaft sind. Weiter kann man, wenn $r_1 > 2r$ ist, ebenso zu (2^b) übergehen u. s. f. Es wiederholen sich unsere früheren Schlüsse, und wir kommen zu folgenden Resultaten: Ist die Gruppe G von der Ordnung r ein Theiler der Gruppe G_1 von der Ordnung r_1 und $r_1 = rq$, dann hat jede zu G gehörige Function φ für die Substitutionen von G_1 genau q Werthe, $\varphi_1, \varphi_2, \cdots \varphi_q$. Die r_1 Substitutionen von G_1 vertheilen sich in q Zeilen von je r Substitutionen

$$(10)\qquad \begin{array}{lllll} s_1 = 1, & s_2\;, & s_3\;, & \cdots & s_r \\ s_1\sigma_2\;, & s_2\sigma_2, & s_3\sigma_2, & \cdots & s_r\sigma_2 \\ s_1\sigma_3\;, & s_2\sigma_3, & s_3\sigma_3, & \cdots & s_r\sigma_3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_1\sigma_q\;, & s_2\sigma_q, & s_3\sigma_q, & \cdots & s_r\sigma_q \end{array}$$

derart, dass die Elemente einer jeden Zeile φ_1 in denselben Werth umwandeln, und dass insbesondere die erste Zeile

*) Mém. de Berl. 1771 = Oeuvres III, p. 359 und p. 374 ff.

alle die Substitutionen enthält, welche φ_1 nicht ändern. Das Schema (10) ist ein Theil des Schemas (2).

Auch hier ist χ_1 rational durch φ_1 darstellbar. Das ergiebt sich genau wie oben der entsprechende Satz; denn in dem Beweise bleibt Alles wie früher, da nur die für den Satz unwesentliche Aenderung der Voraussetzungen eintritt, dass $\chi_1 = \chi_2 = \cdots = \chi_q$, und ebenso $\chi_{q+1} = \cdots = \chi_{2q}$ u. s. w. wird.

Unsere Ueberlegungen zeigen auch: Ist eine Function χ_1 rational durch eine andere φ_1 darstellbar, dann ist der Grad der irreductiblen Gleichung, welcher χ_1 genügt, ein Theiler des Grades derjenigen irreductiblen Gleichung, welcher φ_1 genügt. Denn die Anzahl der Werthe von χ_1 ist $\frac{n!}{r_1} = \frac{n!}{r \cdot q} = \frac{\varrho}{q}$.

Handelt es sich hingegen umgekehrt darum, eine Function φ der enthaltenden Gattung G durch eine Function χ der enthaltenen Gattung G_1 auszudrücken, so kommen wir auf das durch (7) gelöste Problem zurück. Wir setzen wieder die Ordnung von G gleich r, die von G_1 gleich r_1 und nehmen $r_1 = rq$ an. Dann rufen die Substitutionen von G_1 aus $\varphi = \varphi_1$ die q Werthe $\varphi_1, \varphi_2, \cdots \varphi_q$ hervor; ihre symmetrischen Functionen bleiben für G_1 ungeändert und gehören deshalb zur Gattung G_1 oder stehen unter ihr. Jedenfalls lassen sie sich also rational durch χ_1 mit Coefficienten ausdrücken, welche in den x symmetrisch sind. Setzen wir demgemäss

$$\begin{aligned}
\varphi_1 + \varphi_2 + \cdots + \varphi_q &= A_1(\chi_1),\\
\varphi_1\varphi_2 + \varphi_1\varphi_3 + \cdots + \varphi_{q-1}\varphi_q &= A_2(\chi_1),\\
\cdots\cdots\cdots\cdots
\end{aligned}$$

dann wird, wenn wir t als Unbekannte einführen,

$$(7^b)\quad t^q - A_1(\chi_1)t^{q-1} + A_2(\chi_1)t^{q-2} - \cdots \pm A_q(\chi_1) = \Phi_1(t;\chi_1) = 0$$

die gesuchte Gleichung werden, deren Wurzeln $\varphi_1, \varphi_2, \cdots \varphi_q$ sind. Die Irreductibilität dieser Gleichung wird in § 573 bewiesen werden.

Bei den Ueberlegungen, die wir in diesem Paragraphen angestellt haben, tritt also die Gattung G_1 an der Stelle der im vorigen Paragraphen behandelten Gattung der symmetrischen Functionen auf, und insofern ist (7^b) als Verallgemeinerung von (7) zu betrachten. Das Schema (10) ist ein Theil des durch (2), (2^a), $\cdots$ (2^c) gegebenen; umgekehrt ist das Polynom von (7^a)

$$(\varphi - \varphi_1)(\varphi - \varphi_2)\cdots(\varphi - \varphi_q)$$

ein Theiler des zu (7) gehörigen Polynoms, d. h. $\Phi_1(t;\chi_1)$ ist ein Divisor von $\Phi(t)$. Es ist $r \cdot \varrho = r_1 \cdot \varrho_1$, und da r_1 ein Multiplum von r ist, so wird ϱ das gleiche Multiplum von ϱ_1.

§ 541. Die ϱ Wurzeln von (7*) sind die verschiedenen Werthe

$$\varphi_1, \varphi_2, \cdots \varphi_\varrho \qquad (\varrho\cdot r = n!),$$

welche $\varphi = \varphi_1$ unter dem Einflusse sämmtlicher Substitutionen zwischen den $z_1, \cdots z_n$ annehmen kann. Wir haben sie bereits oben als einander conjuge Werthe bezeichnet. Jedem der conjugen Werthe $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ entspricht eine Zeile von Substitutionen des Schemas (2), (2*), $\cdots$. Diese bilden aber mit Ausnahme derjenigen der ersten Zeile G keine Gruppen, wie ja schon daraus hervorgeht, dass keins der übrigen Systeme die Einheit enthält. Wir werden deshalb bei ihrer Bezeichnung auf die Benutzung des Wortes „Gruppe" verzichten müssen und wollen sie als die der Gruppe G conjugen Complexe oder kurz als conjuge Complexe bezeichnen, und schreiben in verständlicher Abkürzung

$$(11) \qquad G;\ G\sigma_2;\ G\sigma_3;\ \cdots\ G\sigma_\varrho.$$

Wir können diesen Begriff nach der Richtung hin erweitern, dass wir auch die Systeme

$$(12) \qquad G;\ \sigma_2' G;\ \sigma_3' G;\ \cdots\ \sigma_\varrho' G,$$

welche aus einer Anordnung (4) entspringen, als conjuge Complexe bezeichnen, trotzdem sie mit der Ueberführung einer Function in ihre conjugen Werthe im Allgemeinen nichts zu thun haben*).

Durch die conjugen Werthe $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ werden conjuge Gattungen charakterisirt. Da φ_2 durch Verwendung von σ_2 auf φ_1 entsteht, so entsteht die zu φ_2 gehörige conjuge Gruppe G_2 dadurch aus $G = G_1$, dass man auch auf alle Elemente der als Cyklen geschriebenen Substitutionen von G_1 die gleiche Substitution σ_2 in Anwendung bringt. Ist also etwa

$$s_i = \begin{pmatrix} z_\alpha \\ z_{i_\alpha} \end{pmatrix}$$

eine Substitution von G und die transformirende Substitution

$$\sigma_2 = \begin{pmatrix} z_\alpha \\ z_{k_\alpha} \end{pmatrix},$$

dann geht daraus für G_2 die Substitution hervor

$$s_i' = \begin{pmatrix} z_{k_\alpha} \\ z_{k_{i_\alpha}} \end{pmatrix}.$$

Das gleiche Resultat ergiebt sich nun aber für die Composition

*) Herr H. Weber gebraucht die Bezeichnung „Nebengruppen".

$$\sigma_2^{-1} s_i \sigma_2 = \begin{pmatrix} z_{k_\alpha} \\ z_\alpha \end{pmatrix} \begin{pmatrix} z_\alpha \\ z_{i_\alpha} \end{pmatrix} \begin{pmatrix} z_\alpha \\ z_{k_\alpha} \end{pmatrix} = \begin{pmatrix} z_{k_\alpha} \\ z_\alpha \end{pmatrix} \begin{pmatrix} z_\alpha \\ z_{i_\alpha} \end{pmatrix} \begin{pmatrix} z_{i_\alpha} \\ z_{k_{i_\alpha}} \end{pmatrix},$$

wodurch wir demnach erkennen, dass G_2 aus

$$(13) \qquad \sigma_2^{-1} s_1 \sigma_2 = 1, \quad \sigma_2^{-1} s_2 \sigma_2, \quad \sigma_2^{-1} s_3 \sigma_2, \cdots \quad \sigma_2^{-1} s_r \sigma_2$$

besteht und kurz durch $G_2 = \sigma_2^{-1} G \sigma_2$ bezeichnet werden kann. Zu

$$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_\varrho$$

gehören demgemäss bezw. die einander conjugen Gruppen

$$G, \; \sigma_2^{-1} G \sigma_2, \; \sigma_3^{-1} G \sigma_3, \cdots \sigma_\varrho^{-1} G \sigma_\varrho.$$

Die Operation, welche von $s_\varkappa$ zu $\sigma^{-1} s_\varkappa \sigma$ oder von einer Gruppe G zu $\sigma^{-1} G \sigma$ führt, wollen wir eine Transformation durch σ nennen. Transformirte Substitutionen und transformirte Gruppen sind einander ähnlich, d. h. sie unterscheiden sich von einander lediglich durch die Bezeichnung der eingehenden Elemente z. Ebenso sind die einander conjugen Functionen einander ähnlich.

Wir wollen diese Begriffe auf unsere einfachsten Gattungen anwenden. Für die symmetrische Gattung ist $r = n!$, $\varrho = 1$; hier giebt es keine conjugen Gattungen.

Ist ferner φ eine zweiwerthige oder alternirende Function, so wird (§ 521)

$$\varphi_1 = S_0 + S_1 \sqrt{D},$$
$$\varphi_2 = S_0 - S_1 \sqrt{D},$$

wobei D die Discriminante der Grössen $z_1, z_2, \cdots z_n$ sein soll, und S_0, S_1 symmetrische Functionen bedeuten. Ein Blick auf die Form von φ_1 und von φ_2 zeigt, dass φ_1 und φ_2 zu derselben Gruppe, der alternirenden, gehören. Das Gleiche ergiebt sich durch die obigen Erwägungen. Denn wenn G die Gruppe aller geraden Substitutionen (§ 520) und σ eine Transposition bedeutet, dann stellt auch $\sigma^{-1} G \sigma$ nur gerade Substitutionen dar. Die beiden conjugen Gattungen von φ_1 und von φ_2 gehören also derselben Gruppe an, d. h. sie fallen zusammen.

Am anderen Ende der Reihe der Substitutionengruppen treten gleiche Verhältnisse ein. Ist φ_1 eine Galois'sche Function, so ist die zugehörige Gruppe gleich 1; jede hieraus transformirte Gruppe ist daher auch gleich 1, und so gehören alle conjugen Werthe derselben Gruppe an. Folglich ist von den conjugen Werthen einer Galois'schen Function jeder als rationale, ganze Function jeder anderen darstellbar, wobei die Coefficienten symmetrische Functionen der Elemente z werden.

Ja, weil jede Gattung unter der Galois'schen Gattung steht, so kann überhaupt eine jede ganze Function der z auf diese Weise ausgedrückt werden.

Wir wollen hiervon sofort einige Anwendungen machen. Ist φ eine Function, die zur erweiterten cyklischen Gruppe (§ 524) gehört, und ist $z_{a_1, a_2, \cdots a_\nu}$ ein beliebiges ihrer Elemente, so wird

$$\chi = z_{a_1, a_2, \cdots a_\nu} + u\varphi(z_{1,1,\cdots}, \cdots)$$

zur Galois'schen Gattung gehören; denn χ bleibt bei unbestimmtem u nur ungeändert, wenn $z_{a_1, \cdots a_\nu}$ und φ ungeändert bleibt; es giebt aber nur die eine Substitution 1, welche zur cyklischen Gruppe gehört und ein Element nicht umstellt. Folglich gehört χ zur Gruppe 1. Demgemäss kann jedes $z_{b_1, b_2, \cdots b_\nu}$ rational durch χ, d. h. durch $z_{a_1, a_2, \cdots a_\nu}$ dargestellt werden, derart dass die Coefficienten cyklische Functionen der Elemente sind. —

Bedeutet ferner φ eine Function, die zur metacyklischen Gruppe gehört (§ 534), und sind z_a, z_b zwei beliebige ihrer Elemente, so wird

$$\chi = u_1 z_a + u_2 z_b + u\varphi(z_1, \cdots z_p)$$

zur Galois'schen Gattung gehören, da nach § 534 nur die Einheitssubstitution der metacyklischen Gruppe mehr als ein Element ungeändert lässt. Demgemäss kann jedes z_c rational durch χ, d. h. durch z_a und z_b dargestellt werden, derart dass die Coefficienten metacyklische Functionen werden, oder: Jede Wurzel einer metacyklischen Gleichung kann als rationale ganze Function zweier beliebigen anderen Wurzeln dargestellt werden, so dass diese Function Coefficienten besitzt, welche zur metacyklischen Gruppe gehören, und also rational bekannt sind.

§ 542. Im vorigen Paragraphen haben wir den Begriff der Transformation einer Substitution oder einer Gruppe durch eine Substitution σ eingeführt. $\sigma^{-1}s\sigma$ heisst die Transformirte oder die Conjuge von s durch σ. Dann ist s die Transformirte von $\sigma^{-1}s\sigma$ durch σ^{-1}. Transformirte oder conjuge Substitutionen sind einander ähnlich. Transformiren wir alle Substitutionen $s_\varkappa$ einer Gruppe durch dieselbe Substitution σ, so bilden die Transformirten wieder eine Gruppe, da man hat:

$$(\sigma^{-1}s_\varkappa\sigma)\cdot(\sigma^{-1}s_\lambda\sigma) = \sigma^{-1}(s_\varkappa s_\lambda)\sigma.$$

Ebenso leicht beweist man, dass alle überhaupt vorhandenen oder auch alle einer Gruppe angehörigen Substitutionen σ', σ'', $\cdots$, welche eine gegebene Substitution s in sich selbst transformiren, für sich eine Gruppe bilden. —

Es sei nun G eine beliebige Gruppe, s_1 eins ihrer Elemente und G' derjenige Theiler von G, welcher s_1 in sich selbst transformirt. Wenn wir (§ 514) $G' = [1, s'_2, s'_3, \cdots s'_m]$ setzen, so wird $s'^{-1}_\alpha s_1 s'_\alpha = s_1$ sein. Ist hingegen t_2 eine nicht in G' vorkommende Substitution von G, so wird $t_2^{-1} s_1 t_2 \neq s_1$ sein; wir setzen diese Transformirte gleich s_2; dann werden alle $s'_\alpha t_2$ dieselbe Conjuge s_2 von s_1 hervorrufen und nur sie. Denn es ist ja

$$(s'_\alpha t_2)^{-1} s_1 (s'_\alpha t_2) = t_2^{-1}(s'^{-1}_\alpha s_1 s'_\alpha) t_2 = t_2^{-1} s_1 t_2 = s_2;$$

und hätte man umgekehrt für irgend eine Substitution ω von G die Relation $\omega^{-1} s_1 \omega = s_2$, dann wäre

$$s_1 = t_2 s_2 t_2^{-1} = t_2 \omega^{-1} s_1 \omega t_2^{-1} = (\omega t_2^{-1})^{-1} s_1 (\omega t_2^{-1}),$$

d. h. es gehörte ωt_2^{-1} zu G', und man hätte

$$\omega t_2^{-1} = s'_\alpha, \quad \omega = s'_\alpha t_2.$$

Hat G mehr Substitutionen als die $2m$ durch s'_α und $s'_\alpha t_2$ repräsentirten, so führen dieselben Schlüsse weiter auf eine neue Conjuge s_3 von s_1 und auf neue m Substitutionen $s'_\alpha t_3$, u. s. f. Daraus ergiebt sich: Die Anzahl μ der zu s_1 conjugen Substitutionen aus G, die durch Transformation mit allen Substitutionen von G entstehen, beträgt einen Theiler der Ordnung der Gruppe G; und die Anzahl m der Sustitutionen, die s_1 in sich selbst transformiren, den conjugen Theiler der Ordnung von G, so dass $m\mu = r$ ist.

Fünfundfünfzigste Vorlesung.

Gattungseigenschaften.

§ 543. Im vorletzten Paragraphen der vorigen Vorlesung haben wir bei der symmetrischen, bei der alternirenden und bei der Galois'schen Gattung bemerkt, dass jedesmal die conjugen Gattungen zusammenfielen oder genauer ausgedrückt, dass es in diesen Fällen gar keine conjugen Gattungen giebt. Wir wollen das hieraus sich ergebende Problem allgemein behandeln.

Gehört $\varphi = \varphi_1$ zur Gruppe G, so gehören die conjugen Werthe von φ_1 nämlich

(1) $$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_\varrho$$

zu den Gruppen, die G ähnlich sind und durch Transformation aus G entstehen,

$$(2) \qquad G, \ \sigma_2^{-1} G \sigma_2, \ \sigma_3^{-1} G \sigma_3, \cdots \ \sigma_\varrho^{-1} G \sigma_\varrho .$$

Giebt es nun ausser der in allen Gruppen (2) vorkommenden Substitution 1 noch andere Substitutionen, die gleichfalls zu allen $\sigma_\alpha^{-1} G \sigma_\alpha$ gehören?

Die Gesammtheit aller vorhandenen bildet jedenfalls wieder eine Gruppe H, da mit s' und s'' auch $s's''$ allen Gruppen angehört. H besitzt die charakteristische Eigenschaft, dass es durch jede Substitution der Elemente z in sich selbst transformirt wird. Denn die Gesammtheit der Gruppen (2) stellt alle Transformirten von G dar und bleibt daher ungeändert, wenn sie durch irgend ein s transformirt wird; und dies muss mit der Gruppe H, die in allen Gruppen (2) enthalten ist, natürlich auch stattfinden.

Die eben aufgestellte, scheinbar allgemeinere Frage ist jetzt also in die umgewandelt, ob es eine Gruppe giebt, die gleich allen ihren conjugen Gruppen ist, d. h. genau in die Frage, welche unseren Ausgangspunkt bildete.

Enthält H irgend eine Substitution, so enthält es auch alle, welche dieser Substitution ähnlich sind; denn diese lassen sich ja aus jener durch eine Transformation herleiten.

Wir betrachten zuvörderst diejenigen Substitutionen von H, die nächst der Einheit möglichst wenige Elemente umsetzen. Da H jeder Transposition gegenüber invariant bleibt, so gilt dasselbe auch dem Complexe H_0 dieser Substitutionen von möglichst wenigen Elementen gegenüber, d. h. H_0 enthält alle einander ähnlichen. Keine derselben kann nun einen Cyklus von mehr als drei Elementen umfassen. Denn wäre etwa eine Substitution mit mehr als drei Elementen eines Cyklus

$$s_1 = (z_1 z_2 z_3 z_4 \cdots) \cdots$$

in H_0 enthalten, so käme auch für $\sigma = (z_1 z_2 z_3)$ die Transformirte vor

$$\sigma^{-1} s_1 \sigma = (z_2 z_3 z_1 z_4 \cdots) \cdots = s_2 ,$$

so dass die Aenderung zwischen s_1 und s_2 lediglich in der Umstellung von z_1, z_2 und z_3 besteht; dann käme aber in H auch das Product der beiden Substitutionen s_1 und s_2^{-1}

$$s_1 s_2^{-1} = (z_2)(z_3 z_1 \cdots)$$

vor; und dies hätte, ohne $= 1$ zu werden, sicher weniger Elemente als s_1, was der Annahme widerspricht, dass s_1 möglichst wenige Elemente in sich fassen soll.

Ebensowenig kann eine Substitution von mehr als drei Elementen auftreten, in welcher ein Cyklus dritter Ordnung vorkommt. Denn aus

$$s_1 = (z_1 z_2 z_3)(z_4 \cdots) \cdots \quad \text{und} \quad \sigma^{-1} s_1 \sigma = (z_1 z_3 z_4)(z_2 \cdots) \cdots = s_2$$

für $\sigma = (z_2 z_3 z_4)$ folgt durch Multiplication, ähnlich wie soeben, dass in H auch das Product

$$s_1 s_2 = (z_3)(z_2 z_4 \cdots) \cdots$$

enthalten ist, also eine Substitution, welche gegen die Annahme weniger Elemente hat als s_1.

Kommt daher überhaupt ein Cykel dritter Ordnung in einer der von uns betrachteten Substitutionen vor, so bildet er für sich selbst schon die Substitution; H enthält dann alle Transformirte dieses einen und deswegen (§ 519) die alternirende Gruppe.

Es ist noch der Fall zu betrachten, dass jede Substitution von H_0 lediglich aus Cyklen zweiter Ordnung besteht. Ist die Zahl n der z_λ grösser als 4, so folgt aus dem Auftreten der beiden Substitutionen

$$s_1 = (z_1 z_2)(z_3 z_4) \cdots, \quad s^{-1} s_1 \sigma = (z_1 z_2)(z_4 z_5) \cdots = s_2$$

für $\sigma = (z_3 z_4 z_5)$ die Existenz von $s_1 \cdot s_2$ in H, und dies hätte, ohne $= 1$ zu sein, weniger als n Elemente als s_1, da ja in

$$s_1 \cdot s_2 = (z_1)(z_2)(z_3 z_5 \cdots) \cdots$$

höchstens $(n - 1)$ Elemente vorhanden sind. Es ist also nur möglich, dass die gesuchten Substitutionen sich als Transpositionen ausweisen, und dann ist H nach § 522 die symmetrische Gruppe.

Ist dagegen $n = 4$, so giebt es für diesen Fall wirklich eine solche Gruppe, nämlich die aus den vier Substitutionen

$$(3) \qquad 1, \ (z_1 z_2)(z_3 z_4), \ (z_1 z_3)(z_2 z_4), \ (z_1 z_4)(z_2 z_3)$$

bestehende, welche sich bei jeder Transposition reproducirt. Diese ist daher als eine Ausnahmegruppe zu bezeichnen. Als eine zu ihr gehörige Function führen wir die sechswerthige Function

$$\psi = (z_1 z_2 + z_3 z_4)(z_1 z_3 + z_2 z_4)$$

an. Wir haben als erstes Resultat das folgende erlangt: Ausser der symmetrischen und der alternirenden Gruppe von beliebig vielen Elementen giebt es allein die Gruppe (3) von vier Elementen, welche durch Transformation mit jeder beliebigen Substitution ihrer Elemente ungeändert bleibt. Nur in diesen Fällen gehören alle conjugen Gattungen derselben

Gruppe an, falls die Gruppe nicht allein aus der identischen Substitution 1 besteht.

Von hier aus ist es leicht, zur allgemeinen Frage wieder zurückzukehren. Da H in G enthalten ist, so kann G auch nur alternirend oder symmetrisch sein, abgesehen von der besonders zu behandelnden Gruppe (3). Für diese kommt aber ausser der alternirenden oder der symmetrischen nur noch eine Gruppe der Ordnung 8 in Frage. Eine solche wird in der That durch das folgende G gegeben, dessen Transformirte ebenfalls angeführt werden sollen:

$$(4) \qquad \begin{array}{l} 1,\ (z_1z_2)(z_3z_4),\ (z_1z_3)(z_2z_4),\ (z_1z_4)(z_2z_3), \\ (z_1z_2z_3z_4),\ (z_1z_3),\ (z_1z_4z_3z_2),\ (z_2z_4). \end{array} \qquad (G)$$

$$\begin{array}{l} 1\ \ (z_1z_2)(z_3z_4),\ (z_1z_3)(z_2z_4),\ (z_1z_4)(z_2z_3), \\ (z_1z_2z_4z_3),\ (z_1z_4),\ (z_2z_3),\ (z_1z_3z_4z_2). \end{array} \qquad \begin{array}{l} (\sigma_2^{-1}G\sigma_2) \\ \sigma_2=(z_3z_4) \end{array}$$

$$\begin{array}{l} 1,\ (z_1z_2)(z_3z_4),\ (z_1z_3)(z_2z_4),\ (z_1z_4)(z_2z_3), \\ (z_1z_3z_2z_4),\ (z_1z_4z_2z_3),\ (z_1z_2),\ (z_3z_4). \end{array} \qquad \begin{array}{l} (\sigma_3^{-1}G\sigma_3) \\ \sigma_3=(z_2z_3) \end{array}$$

Als einfachste zugehörige Functionen führen wir die folgenden conjugen an, deren Wichtigkeit schon bei der Lösung der Gleichungen vierten Grades heraustrat:

$$(5) \qquad \varphi_1 = z_1z_3 + z_2z_4, \quad \varphi_2 = z_1z_4 + z_2z_3, \quad \varphi_3 = z_1z_2 + z_3z_4.$$

Ausser den symmetrischen, den alternirenden und den Functionen der Gattungen (3) und (4) giebt es keine anderen, deren conjuge Werthe sämmtlich für eine und dieselbe Substitution ungeändert bleiben. Dieser Satz bleibt auch dann richtig, wenn man nicht sämmtliche conjugen Werthe der Function betrachtet, sondern nur die durch Transformationen mit geraden Substitutionen hervorgerufenen. Der Beweis ist bereits dadurch geführt, dass die oben benutzten transformirenden Substitutionen σ sämmtlich die Form $(z_\alpha z_\beta z_\gamma)$ haben und also der alternirenden Gruppe angehören.

§ 544. Hieraus lässt sich ein weiterer interessanter Satz ableiten. Alternirende Functionen, welche von der Form sind

$$\varphi = S\cdot\sqrt{\varDelta},$$

haben die Eigenschaft, selbst zweiwerthig zu sein, während eine Potenz von ihnen, die zweite nämlich, unter der Gattung steht und einwerthig wird. Wir wollen die Frage erörtern: Welche mehrwerthigen Functionen haben die Eigenschaft, dass eine ihrer Potenzen einwerthig wird?

Ist $\varphi^\varkappa = S$ einwerthig, dann unterscheiden sich die conjugen Werthe von φ nur durch $\varkappa^{te}$ Einheitswurzeln $\omega, \omega^2, \cdots$ als Factoren, da $\varphi = S^{\frac{1}{\varkappa}}$ wird. Diese conjugen Werthe $\varphi, \omega^\alpha\varphi, \omega^\beta\varphi, \cdots$ gehören deshalb sämmtlich zu derselben Gruppe; denn die constanten Factoren $\omega^\alpha, \omega^\beta, \cdots$ sind dabei einflusslos, weil bei einer Substitution gleichzeitig φ und $\omega^\alpha\varphi$ ungeändert bleiben. Damit sind wir auf die Untersuchungen des vorigen Paragraphen zurückgeführt worden.

Ausser den ein- und den zweiwerthigen Functionen können daher höchstens noch solche Functionen von vier Variablen in Frage kommen, die zur Gruppe (3) gehören. Da (3) von der Ordnung 4 ist, so müsste es eine sechswerthige Function geben, deren sechste Potenz, und also müsste es, wenn man ihr Quadrat betrachtet, eine dreiwerthige Function geben, deren dritte Potenz symmetrisch wird. Das könnte nur stattfinden, wenn eine Gruppe von vier Elementen von der Ordnung 8 vorhanden wäre, welche mit ihren conjugen Gruppen übereinstimmt; und da dies nach dem vorigen Paragraphen nicht der Fall ist, so giebt es keine derartige Function. Damit ist bewiesen: Es giebt ausser den alternirenden Functionen $S\cdot\sqrt{\Delta}$ keine anderen mehrwerthigen Functionen, von denen eine Potenz einwerthig wird.

Giebt es nun vielleicht Functionen, welche mehr als zweiwerthig sind und von denen eine Potenz zweiwerthig ist? Wir machen dieselben Schlüsse. Ist $\varphi^\varkappa$ zweiwerthig, so bleibt es für alle Substitutionen der alternirenden Gruppe ungeändert (§ 521). Unter dem Einflusse der geraden Substitutionen kann also φ nur Werthe $\omega^\alpha\varphi, \omega^\beta\varphi, \cdots$ annehmen, bei denen ω eine $\varkappa^{te}$ Einheitswurzel bedeutet. Alle diese Werthe gehören nun zu derselben Gruppe; d. h. die Gruppe von φ ändert sich unter dem Einflusse der Transformation durch irgend welche gerade Substitution nicht. Nach der Schlussbemerkung des vorigen Paragraphen kann also φ, da es weder symmetrisch noch alternirend ist, nur zur Ausnahmegruppe (3) gehören, falls es überhaupt existirt; und nur eine zu (3) gehörige sechswerthige Function kann eine zweiwerthige dritte Potenz haben. In der That giebt es auch solche. Bedeutet ω eine primitive dritte Einheitswurzel, so bilden wir aus den Functionen (5) die Summe

$$\psi_1 = (z_1 z_2 + z_3 z_4) + \omega(z_1 z_3 + z_2 z_4) + \omega^2(z_1 z_4 + z_2 z_3);$$

wenden wir auf sie die $6 \cdot 4$ Substitutionen zwischen z_1, z_2, z_3, z_4 an, dann entstehen die fünf zu ψ_1 conjugen Functionen

$$\psi_2 = (z_1 z_3 + z_2 z_4) + \omega(z_1 z_4 + z_2 z_3) + \omega^2(z_1 z_2 + z_3 z_4),$$
$$\psi_3 = (z_1 z_4 + z_2 z_3) + \omega(z_1 z_2 + z_3 z_4) + \omega^2(z_1 z_3 + z_2 z_4),$$
$$\psi_4 = (z_1 z_2 + z_3 z_4) + \omega(z_1 z_4 + z_2 z_3) + \omega^2(z_1 z_3 + z_2 z_4),$$
$$\psi_5 = (z_1 z_4 + z_2 z_3) + \omega(z_1 z_3 + z_2 z_4) + \omega^2(z_1 z_2 + z_3 z_4),$$
$$\psi_6 = (z_1 z_3 + z_2 z_4) + \omega(z_1 z_2 + z_3 z_4) + \omega^2(z_1 z_4 + z_2 z_3).$$

Hier ist nun
$$\psi_1 = \omega\psi_2 = \omega^2\psi_3; \quad \psi_4 = \omega\psi_5 = \omega^2\psi_6,$$
so dass wir für die dritten Potenzen der sechs ψ, wie behauptet wurde, nur zwei verschiedene Werthe erhalten
$$\psi_1^3 = \psi_2^3 = \psi_3^3; \quad \psi_4^3 = \psi_5^3 = \psi_6^3.$$

§ 545. Wir werden durch diese Untersuchungen zu einer allgemeineren Frage geführt: Wann wird die p^{te} Potenz einer $p \cdot \varrho$-werthigen Function φ, die zur Gattung H gehört, eine ϱ-werthige Function, die zur Gattung G gehört?

Jede Substitution, welche φ nicht ändert, d. h. zur Gruppe H gehört, lässt auch φ^p ungeändert und gehört daher auch zur Gruppe G. Es steht daher φ^p unter der Gattung von φ, und G ist ein Vielfaches von H. Unsere Frage ist demnach aus folgendem Grunde wichtig. Nach § 540 kann man allgemein den Uebergang von irgend einer Function χ der Gattung G zu irgend einer Function ψ der Gattung H durch die Auflösung einer Gleichung p^{ten} Grades bewirken, deren Coefficienten in χ rational sind. Wenn man nun in unserem Falle zunächst von χ zu φ^p geht, was auf rationalem Wege geschehen kann, und ebenso von ψ zu φ, dann erkennt man, dass die Gleichung p^{ten} Grades (7^{b}) § 540 zwischen χ und ψ durch eine binomische Gleichung p^{ten} Grades ersetzt werden kann. Dadurch ist demnach das Problem ausserordentlich vereinfacht.

Wir wollen voraussetzen, dass p eine Primzahl bedeute. Das ist keine Einschränkung; denn wenn die $(pq)^{\text{te}}$ Potenz einer $(pq) \cdot \varrho$-werthigen Function ϱ-werthig wird, so gilt von ihrer q^{ten} Potenz die eben vorausgesetzte Eigenschaft, dass eine Primzahlpotenz von ihr weniger Werthe besitzt als sie selbst.

Es sei also die zur Gruppe H gehörige Function φ eine $p \cdot \varrho$-werthige Function, während φ^p nur ϱ Werthe besitzt, so dass die zu φ^p gehörige Gruppe G eine p mal höhere Ordnung hat als die zu φ gehörige Gruppe H. Nun sei σ irgend eine Substitution von G, die in H nicht vorkommt. Bilden wir $H \cdot \sigma$, d. h. den Complex aller rechtsseitig mit σ multiplicirten Substitutionen von H, so kommen alle diese in G vor und sind unter sich und von den Substitutionen von H

verschieden. Unter ihnen findet sich σ^2 nicht, da aus $\sigma^2 = s_\alpha \sigma$ folgen würde $\sigma = s_\alpha$. Wir bilden hiermit weiter $H \cdot \sigma^2$ und dann ebenso $H \cdot \sigma^3, \cdots$ bis zu $H \cdot \sigma^{\pi-1}$, falls σ^π nämlich die erste in H vorkommende Potenz von σ ist.

Da σ nicht zu H gehört, so wird es φ_1 in einen Werth φ_2 transformiren, der von φ_1 verschieden ist; da aber $\varphi_1^p = \varphi_2^p$, so folgt $\varphi_2 = \omega\varphi_1$, wobei ω primitive p^{te} Einheitswurzel ist. Somit transformirt σ^2 weiter φ_1 in $\varphi_3 = \omega^2\varphi_1$ u. s. f. und σ^π transformirt es in $\varphi_1\omega^\pi$. Dies muss wieder mit φ_1 zusammenfallen, weil σ^π zu H gehört; demnach ist π ein Vielfaches von p. Andererseits ist $\omega^p\varphi_1 = \varphi_1$, d. h. σ^p gehört bereits zu H. Das lässt erkennen, dass p ein Vielfaches von π, und da p eine Primzahl ist, dass $p = \pi$ wird; d. h.: Ist σ irgend welche Substitution von G, die nicht selbst zu H gehört, dann gehört σ^p zu H. — Die Gruppe G entsteht, wenn man mit den Substitutionen von H noch σ combinirt.

Ferner haben $\varphi_1, \varphi_1\omega, \varphi_1\omega^2, \cdots$ dieselbe Gruppe, d. h. die transformirte Gruppe $\sigma^{-1}H\sigma$ stimmt für jede Substitution σ aus G mit der ursprünglichen Gruppe H überein.

Wenn umgekehrt jede p^{te} Potenz σ^p einer beliebigen Substitution σ aus G zum Theiler H gehört, und wenn

$$\sigma^{-1}H\sigma = H \tag{6}$$

ist, dann kann man eine zu H gehörige Function construiren, deren p^{te} Potenz zu G gehört. Es sei nämlich ψ irgend eine zur Gattung H gehörige Function, und die Transformation mit $1, \sigma, \sigma^2, \cdots \sigma^{p-1}$ möge aus ihr die Werthe $\psi_1, \psi_2, \psi_3, \cdots \psi_p$ hervorrufen, die dann wegen (6) zu derselben Gruppe H gehören. Wir bilden hierauf mit Hülfe einer primitiven p^{ten} Einheitswurzel ω die Resolvente

$$\varphi_1 = \psi_1 + \omega\psi_2 + \omega^2\psi_3 + \cdots + \omega^{p-1}\psi_p, \tag{7}$$

dann wird, da die Wirkung von σ^2 auf ψ_1 gleich der von σ auf ψ_2 ist u. s. f., die Verwendung von $\sigma, \sigma^2, \cdots$ daraus

$$\begin{aligned} \varphi_2 &= \psi_2 + \omega\psi_3 + \omega^2\psi_4 + \cdots + \omega^{p-1}\psi_1 = \omega^{-1}\varphi_1, \\ \varphi_3 &= \psi_3 + \omega\psi_4 + \omega^2\psi_5 + \cdots + \omega^{p-1}\psi_2 = \omega^{-2}\varphi_1, \\ &\cdots\cdots\cdots\cdots \end{aligned} \tag{8}$$

hervorrufen, woraus nun wirklich

$$\varphi_1^p = \varphi_2^p = \varphi_3^p = \cdots = \varphi_{p-1}^p \tag{9}$$

folgt.

Die oben festgestellte Beziehung der Gruppen H und G zu einander reicht also vollkommen aus. Wir müssen uns aber hüten, dieses

Resultat als eine definitive Lösung des gestellten Problems anzusehen; es ist lediglich eine Umformung desselben aus dem Gebiete der rationalen Functionen in dasjenige der Substitutionentheorie, in welchem freilich die Beantwortung der Frage häufig bequemer sich gestaltet.

Die Structur von (7) zeigt, dass die Gleichung, deren Wurzeln $\varphi_1, \varphi_2, \cdots \varphi_p$ sind, eine cyklische Gleichung wird; zugleich giebt sie an, auf welche Weise man mit Hülfe einer Substitution σ die cyklische Anordnung der Werthe φ finden kann.

§ 546. Unter den Gruppen, die wir bisher studiert haben, nehmen die der einwerthigen und die der zweiwerthigen Functionen bedeutsame Stellen ein; sie liefern diejenigen Gattungen, bei denen die Anzahl der conjugen Gattungen so klein als möglich wird. Für jede Anzahl n der Variablen z bestehen solche Gattungen mit den Werthezahlen $\varrho = 1$ und $\varrho = 2$. Wir wollen untersuchen, welches wohl die nächsten sich daran anschliessenden Gattungen mit möglichst geringem ϱ sind. Es wird sich bei dieser Untersuchung herausstellen, dass, wenn $n > 4$ ist, keine Gattung mit mehr als zwei und weniger als n conjugen Werthen besteht*).

Hat nämlich eine Function φ die ϱ conjugen Werthe

$$(10) \qquad \varphi_1, \varphi_2, \varphi_3, \cdots \varphi_\varrho,$$

und wendet man auf diese Reihe alle $n!$ Substitutionen s_i der symmetrischen Gruppe der z an, so erhält man $n!$ Anordnungen der Reihe der Functionen

$$(11) \qquad \varphi_{i_1}, \varphi_{i_2}, \varphi_{i_3}, \cdots \varphi_{i_\varrho},$$

welche man als ebensoviele Permutationen der Anordnung (10) auffassen kann. Wir wollen also diese Umwandlungen in der Aufeinanderfolge

$$(12) \qquad v_i = \begin{pmatrix} \varphi_1, & \varphi_2, & \cdots & \varphi_\varrho \\ \varphi_{i_1}, & \varphi_{i_2}, & \cdots & \varphi_{i_\varrho} \end{pmatrix}$$

als Substitutionen v_i der ϱ Elemente φ ansehen. Nun giebt es an verschiedenen Substitutionen v_i bei ϱ Elementen grade $\varrho!$; ist also

*) Ruffini (Teorica di Equaz. Bologna 1799) beweist, dass für $n = 5$, $\varrho < 5$ nur $\varrho = 2$ sein kann; Abatti (Mem. della Soc. Ital. 10), dass für $n, \varrho \leqq 5$ nur $\varrho = 2$ sein könne. Cauchy (J. d. l'Éc. polyt. cah. 10, p. 17) erweitert diese Sätze dahin, dass für $\varrho > 2$ auch $\varrho > p$ sein müsse, wo p die grösste Primzahl $< n$ bedeutet. Der obige allgemeine Satz wurde zuerst von Bertrand bewiesen (J. d. l'Éc. polyt. (1845) p. 131); die Ausnahme für $n = 4$ wurde von Serret festgestellt (J. d. M. 15 (1850) p. 45). Der im Texte gegebene Beweis stammt von Kronecker. — Weitere Beweise sowie tiefere Untersuchungen finden sich in meiner Substitutionentheorie, sowie in C. Jordan's „Traité des substitutions".

$\varrho < n$, so wird die Anzahl der v_i kleiner als die Anzahl der Substitutionen s_i. Daher giebt es mindestens zwei Substitutionen der z, etwa s_i und s_k, welche von einander verschieden sind, trotzdem aber dieselben Umstellungen der φ unter einander hervorrufen, indem für sie $v_i = v_k$ wird. In diesem Falle muss $s_i s_k^{-1}$ die Reihe $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ zuerst in $\varphi_{i_1}, \varphi_{i_2}, \cdots \varphi_{i_\varrho}$ und diese dann rückwärts in $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ umwandeln. Es bleibt demnach unter dem Einflusse des von der Einheit verschiedenen $s_i s_k^{-1}$ jedes Glied der Reihe (11) an seiner Stelle, d. h. $s_i s_k^{-1}$ gehört jeder der Gruppen der conjugen Functionen $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ an. Nach § 543 ist dies jedoch nur dann möglich, wenn $n = 4$ ist; d. h. für $n > 4$ ist $\varrho \geqq n$. Für $n = 4$ dagegen haben wir wirklich eine Gattung kennen gelernt, für welche $\varrho = 3$ ist; zu ihr gehören die conjugen Functionen

$$\varphi_1 = z_1 z_2 + z_3 z_4, \quad \varphi_2 = z_1 z_3 + z_2 z_4, \quad \varphi_3 = z_1 z_4 + z_2 z_3.$$

§ 547. Die nächste in Betracht kommende Frage ist somit die Frage nach den n-werthigen Functionen von n Elementen, $\varrho = n$; $r = (n-1)!$. Es giebt solche für jedes n; denn z_1 ist ja selbst Repräsentant einer Gattung, deren n conjuge Werthe durch $z_1, z_2, \cdots z_n$ gegeben sind. Wir wollen zeigen, dass für $n \neq 6$ dadurch die einzige vorhandene Gattung geliefert wird, während für $n = 6$ ausserdem noch als eine Ausnahmegattung eine Function von sechs Werthen besteht.

Ist $\varrho = n$, so giebt es $n!$ Substitutionen (12), und diese müssen nach dem vorigen Paragraphen sämmtlich von einander verschieden sein. Es müssen also zwei beliebigen verschiedenen s_i, s_k auch zwei verschiedene v_i, v_k zugeordnet sein und umgekehrt. Die v_i werden dabei dann die Gesammtheit aller $\varrho! = n!$ Substitutionen zwischen den φ darstellen, wie die s_i diejenige aller Substitutionen zwischen den s.

Entspricht einem s_i ein v_i, so entspricht dem s_i^2 das v_i^2; ist also s_i eine Transposition, so wird v_i^2 der Einheit entsprechen, d. h. 1 sein. Folglich kann einer Transposition s_i nur eine Substitution v_i von der zweiten Ordnung entsprechen. Demgemäss unterscheiden wir zwei Fälle:

I) Einem $s_i = (z_\alpha z_\beta)$ entspricht ein $v_i = (\varphi_\gamma \varphi_\delta)$,

II) Keinem $s_i = (z_\alpha z_\beta)$ entspricht ein $v_i = (\varphi_\gamma \varphi_\delta)$.

Wir betrachten zunächst den ersten Fall, d. h. den, in welchem die Transposition zweier Elemente z_α, z_β in (10) auch nur eine Transposition zweier Elemente φ_γ, φ_δ hervorbringt. Dann entspricht, was auch s_α bedeuten möge, dem

$$s_\alpha^{-1} s_i s_\alpha \quad \text{das} \quad v_\alpha^{-1} v_i v_\alpha$$

und umgekehrt. Das erstere liefert nun alle Transpositionen der z, wenn s_α geeignete Elemente durchläuft, und das zweite daher alle Transpositionen der v. Diese entsprechen sich sonach gegenseitig eindeutig.

Ebenso folgt, wenn den Transpositionen

$$s_i = (z_\alpha z_\beta), \quad s_k = (z_\alpha z_\gamma) \quad \text{entsprechen} \quad v_i = (\varphi_\gamma \varphi_\delta), \quad v_k = (\varphi_\varepsilon \varphi_\zeta),$$

dass dem Cyklus dritter Ordnung

$$s_i s_k = (z_\alpha z_\beta z_\gamma) \quad \text{entspricht} \quad v_i v_k.$$

Da aber $(s_i s_k)^3 = 1$ ist, so muss gleichfalls $(v_i v_k)^3 = 1$ eintreten. Nun hat $v_i v_k$ höchstens vier Elemente φ; und daraus ist ersichtlich, dass $v_i v_k$ eine cyklische Substitution dritter Ordnung wird. Das ist nur möglich, wenn in v_i und v_k ein gemeinsames Element vorkommt, wenn also, da es auf die Indicesbezeichnung nicht ankommt,

$$v_i = (\varphi_\gamma \varphi_\delta), \quad v_k = (\varphi_\gamma \varphi_\varepsilon)$$

ist. Betrachtet man weiter $s_m = (z_\beta z_\gamma)$, dann folgt ebenso $v_m = (\varphi_\delta \varphi_\varepsilon)$ u. s. f. Man kann also, wenn man die Indicesbezeichnung der φ passend abändert, allgemein folgende Zuordnung treffen: Jedem

$$s_i = (z_\alpha z_\beta) \quad \text{entspricht} \quad v_i = (\varphi_\alpha \varphi_\beta).$$

Dann wird aus jeder Substitution der z die entsprechend zugeordnete der φ gefunden, indem man einfach in jener statt jedes Zeichens z das Zeichen φ setzt, ohne Indices oder Cyklen zu ändern.

Hieraus ist ersichtlich, dass diejenigen Substitutionen der φ das Element φ_1 nicht ändern, welche die symmetrische Gruppe der $\varphi_2, \varphi_3, \cdots \varphi_\varrho$ bilden, d. h. φ_1 bleibt bei denjenigen s_α ungeändert, welche die symmetrische Gruppe der $z_2, z_3, \cdots z_\varrho$ ausmachen und also z_1 nicht umschliessen. Folglich gehört z_1 zu derselben Gattung wie φ_1.

Dies ist der erste, allgemeine Fall für $\varrho = n$. Er entspringt aus der Annahme I.

Gehen wir nunmehr zu dem Falle II über, so können wir als einander entsprechend annehmen die beiden Substitutionen

$$s_i = (z_\alpha z_\beta) \quad \text{und} \quad u_i = (\varphi_a \varphi_b)(\varphi_c \varphi_d) \cdots.$$

Hieraus folgern wir, genau wie im vorigen Falle, dass allen Transpositionen der z alle diejenigen Substitutionen der φ entsprechen, welche mit u_i von gleichem Typus sind, d. h. welche u_i ähnlich sind. Damit also eine solche Zuordnung möglich sei, muss es von beiden Sorten von Substitutionen in der symmetrischen Gruppe von $n = \varrho$ Elementen gleich viele geben. Nun existirt in ihr an Substitutionen vom Typus

(A) $(z_\alpha z_\beta)$ die Anzahl $\frac{1}{2}n(n-1)$,

(B) $(z_\alpha z_\beta)(z_\gamma z_\delta)$ „ „ $\frac{1}{2!}\frac{1}{2^2}n(n-1)(n-2)(n-3)$,

(C) $(z_\alpha z_\beta)(z_\gamma z_\delta)(z_\eta z_\vartheta)$ „ „ $\frac{1}{3!}\frac{1}{2^3}n(n-1)\cdots(n-4)(n-5)$,

(D) $(z_\alpha z_\beta)(z_\gamma z_\delta)(z_\eta z_\vartheta)(z_\iota z_\varkappa)$ „ „ $\frac{1}{4!}\frac{1}{2^4}n(n-1)\cdots(n-6)(n-7)$,

. . . .

wie man leicht erkennt. Es könnte deshalb u_i nur dann vom Typus (B) sein, wenn für ein ganzes, positives n

$$\frac{1}{2}n(n-1) = \frac{1}{2!}\frac{1}{2^2}n(n-1)(n-2)(n-3), \quad \text{d. h.} \quad (n-2)(n-3) = 4$$

wäre, was nicht möglich ist. Ferner könnte u_i nur dann vom Typus (C) sein, wenn für ein ganzes, positives n

$$\frac{1}{2}n(n-1) = \frac{1}{3!}\frac{1}{2^3}n(n-1)\cdots(n-4)(n-5),$$

$$(n-2)(n-3)(n-4)(n-5) = 24$$

wäre. Diese Gleichung hat nur die eine brauchbare Wurzel $n = 6$.

Damit sind alle Möglichkeiten erschöpft; denn damit (D) oder eine der weiteren Möglichkeiten erfüllt wäre, müsste eine Zahl $4!\,2^3$, oder $5!\,2^4$, oder $6!\,2^5, \cdots$ als Product von sechs, oder acht, oder zehn, $\cdots$ aufeinander folgenden ganzen Zahlen darstellbar sein. Das ist nicht möglich. Dividirt man nämlich durch $6!$ oder $8!$ oder $10!$ u. s. w., so erscheinen einerseits ganze Zahlen und andrerseits die echten Brüche

$$2\cdot\frac{2^2}{5\cdot 6},\quad 2\cdot\frac{2^3}{6\cdot 7\cdot 8},\quad 2\cdot\frac{2^4}{7\cdot 8\cdot 9\cdot 10},\ \cdots.$$

Es fragt sich deshalb nur noch, ob für $\varrho = n = 6$ wirklich eine Ausnahmegattung vorhanden ist. Kommt eine solche vor, so ist dies allein bei einer Function φ möglich, bei welcher sich Substitutionen der z und der φ von folgenden Typen

(13) $$s_1 = (z_1 z_2) \quad \text{und} \quad u_1 = (\varphi_1\varphi_2)(\varphi_3\varphi_4)(\varphi_5\varphi_6)$$

entsprechen.

Wir fragen jetzt, was für ein u_2 einem $s_2 = (z_3 z_4)$ entsprechen kann, welches mit s_1 kein z gemeinsam hat. Da $s_1 s_2 = (z_1 z_2)(z_3 z_4)$ ist, und da diesem Typus gemäss unserer schematischen Uebersicht aus Gründen der Gleichheit der Anzahlen nur wieder eine Substitution von gleichem Typus entsprechen kann, so ist $u_1\cdot u_2$ auch von der Form $(\varphi_\alpha\varphi_\beta)(\varphi_\gamma\varphi_\delta)$. Wir müssen also untersuchen, wann aus $u_1\cdot u_2$ zwei Elemente φ herausfallen, die in u_1 und in u_2 einzeln vorkommen.

Soll etwa φ_5 herausfallen, so zeigt die Productbildung, dass u_2 den Cyklus $(\varphi_5\varphi_6)$ hat, und da man die Elemente φ noch beliebig benennen kann, so dürfen wir als einander entsprechend setzen

$$s_2 = (z_3 z_4) \quad \text{und} \quad u_2 = (\varphi_a\varphi_b)(\varphi_c\varphi_d)(\varphi_5\varphi_6).$$

Wegen der Möglichkeit, die Zahlen a, b, c, d auf $1, 2, 3, 4$ beliebig zu vertheilen, mit der Einschränkung, dass a, b nicht gleichzeitig $1, 2$ oder $3, 4$ sein dürfen, kann man ohne Beschränkung setzen

$$(14) \qquad s_2 = (z_3 z_4) \quad \text{und} \quad u_2 = (\varphi_1\varphi_3)(\varphi_2\varphi_4)(\varphi_5\varphi_6).$$

Dieselben Schlüsse gelten für das u_3, welches der Substitution $s_3 = (z_5 z_6)$ zugeordnet ist, d. h. u_3 hat mit u_1 und mit u_2 je einen Cyklus zweier Elemente gemeinsam. Das kann nur $(\varphi_5\varphi_6)$ sein; also wird

$$(15) \qquad s_3 = (z_5 z_6) \quad \text{und} \quad u_3 = (\varphi_1\varphi_4)(\varphi_2\varphi_3)(\varphi_5\varphi_6).$$

Die Construction des zu $s_4 = (z_1 z_3)$ gehörigen u_4 gründen wir darauf, dass die Producte $s_1 s_4 = (z_1 z_2 z_3)$ und $s_2 s_4 = (z_1 z_3 z_4)$ von dritter Ordnung sind, und dass demgemäss das Gleiche auch bei $u_1 u_4$ und $u_2 u_4$ eintreten muss. Es könnte nun eins dieser Producte ein Cyklus dritter Ordnung werden, falls bei der Multiplication drei Elemente verschwinden würden. Wir sahen aber, dass bei der Form von $u_1, u_2, \cdots$ Elemente nur verschwinden, wenn Cykel gemeinsam sind; sollen drei Elemente verschwinden, so kämen zwei gleiche Cyklen vor, und die u wären identisch. Es muss also $u_1 u_4$ und $u_2 u_4$ aus je zwei Cyklen dritter Ordnung bestehen. Hat nun u_4 mit u_1 und u_2 keinen Cyklus gemeinsam, dann bleiben für u_4 die vier Möglichkeiten

$$u_4 = (\varphi_1\varphi_4)(\varphi_2\varphi_5)(\varphi_3\varphi_6), \quad u_4' = (\varphi_1\varphi_5)(\varphi_2\varphi_3)(\varphi_4\varphi_6),$$
$$u_4'' = (\varphi_1\varphi_4)(\varphi_2\varphi_6)(\varphi_3\varphi_5), \quad u_4''' = (\varphi_1\varphi_6)(\varphi_2\varphi_3)(\varphi_4\varphi_5).$$

Nun ändert sich in (13), (14), (15) nichts, wenn man φ_5 mit φ_6 vertauscht. Dadurch geht u_4'' in u_4 und u_4''' in u_4' über; man kann sich also auf die Möglichkeiten u_4 und u_4' beschränken.

Transformiren wir ferner (13), (14), (15), s_4 und u_4' durch s_2 und bezw. u_2, dann ändern sich nur s_4 und u_4' und diese geben

$$(z_1 z_4) \quad \text{und} \quad (\varphi_1\varphi_4)(\varphi_2\varphi_5)(\varphi_3\varphi_6) = u_4.$$

Bezeichnet man dann also schliesslich die z so, dass man z_3 und z_4 vertauscht, so kommt man auch von dem Falle u_4' durch die eben betrachteten Umwandlungen auf

$$(16) \qquad s_4 = (z_1 z_3) \quad \text{und} \quad u_4 = (\varphi_1\varphi_4)(\varphi_2\varphi_5)(\varphi_3\varphi_6).$$

Durch Transformation von (16) mit s_2 und bezw. u_2 findet man weiter

$$(17) \qquad s_5 = (z_1 z_4) \quad \text{und} \quad u_5 = (\varphi_1\varphi_5)(\varphi_2\varphi_3)(\varphi_4\varphi_6).$$

Um das u_6 zu finden, welches dem $s_6 = (z_1 z_5)$ entspricht, bedenken wir, dass $s_1 s_6$, $s_3 s_6$, $s_4 s_6$, $s_5 s_6$ und deshalb auch $u_1 u_6$, $u_3 u_6$, $u_4 u_6$, $u_5 u_6$ dritter Ordnung sind. Nach den eben angestellten Ueberlegungen kann u_6 mit u_1, u_3, u_4, u_5 keinen Cyklus gemeinsam haben; es bleiben demnach für u_6 nur die beiden Möglichkeiten

$$u_6 = (\varphi_1\varphi_3)(\varphi_2\varphi_6)(\varphi_4\varphi_5) \quad \text{oder} \quad u_6' = (\varphi_1\varphi_6)(\varphi_2\varphi_4)(\varphi_3\varphi_5).$$

Transformirt man dies durch die Substitutionen (15), so findet man als dem $s_7 = (z_1 z_6)$ entsprechend

$$u_7 = (\varphi_1\varphi_6)(\varphi_2\varphi_4)(\varphi_3\varphi_5) = u_6' \quad \text{oder} \quad u_7' = (\varphi_1\varphi_3)(\varphi_2\varphi_6)(\varphi_4\varphi_5) = u_6.$$

Es ist also gleichgültig, welche der beiden Möglichkeiten man für u_6 wählt, da Vertauschung von z_5 und z_6 untereinander eine jede auf die andere transformiren wird. Wir setzen somit

$$(18) \qquad s_6 = (z_1 z_5) \quad \text{und} \quad u_6 = (\varphi_1\varphi_3)(\varphi_2\varphi_6)(\varphi_4\varphi_5),$$

$$(19) \qquad s_7 = (z_1 z_6) \quad \text{und} \quad u_7 = (\varphi_1\varphi_6)(\varphi_2\varphi_4)(\varphi_3\varphi_5).$$

Durch die Formeln (13) bis (19) ist die Gruppe bestimmt, falls sie widerspruchsfrei existirt. Diejenigen Substitutionen s, deren zugehörige u das Element φ_6 nicht umsetzen, bilden die zu φ_6 gehörige Gruppe G_6. Diese muss die Ordnung $r = 120$ haben.

Nun ist

$$\begin{aligned}
u_1u_4u_5u_6u_7 &= (\varphi_1\varphi_5)(\varphi_2\varphi_4\varphi_3); & s_1s_4s_5s_6s_7 &= (z_1z_2z_3z_4z_5z_6) = t_1,\\
u_1u_4u_7u_5 &= (\varphi_1\varphi_2\varphi_3\varphi_4\varphi_5); & s_1s_4s_7s_5 &= (z_1z_2z_3z_6z_4) = t_2,\\
u_5u_6u_1 &= (\varphi_1\varphi_3\varphi_5\varphi_4); & s_5s_6s_1 &= (z_1z_4z_5z_2) = t_3.
\end{aligned}$$

Man erkennt leicht, dass t_2 von allen Potenzen von t_1, und dass t_3 von allen Producten $t_1^\alpha t_2^\beta$ verschieden ist. Alle $6\cdot 5\cdot 4 = 120$ Substitutionen

$$(20) \quad t_1^\alpha t_2^\beta t_3^\gamma \qquad (\alpha = 1, 2, \cdots 6;\ \beta = 1, 2, \cdots 5;\ \gamma = 1, 2, \cdots 4)$$

sind von einander verschieden; G_6 hat also mindestens die Ordnung 120.

Andrerseits bleibt z. B.*) die Function

$$\varphi_6 = (z_1z_2 + z_3z_4 + z_5z_6)(z_1z_3 + z_2z_5 + z_4z_6)(z_1z_4 + z_2z_6 + z_3z_5)$$
$$(z_1z_5 + z_2z_4 + z_3z_6)(z_1z_6 + z_2z_3 + z_4z_5)$$

für t_1, t_2, t_3 und also für die 120 Substitutionen $t_1^\alpha t_2^\beta t_3^\gamma$ ungeändert; aber auch nur für diese, da φ_6, wie man leicht sieht, sechs Werthe hat, und $6 \cdot 120 = 6!$ ist. Folglich geben die Substitutionen (20) eine Gruppe G_6 mit $n = 6$, $\varrho = 6$ als Ausnahmegruppe.

---

*) Vgl. hierzu: Dziobek, Arch. f. Math. 68, p. 226 u. 230; Hölder, Math. Ann. 46, p. 333 ff.

§ 548. Wir sahen oben § 540, (8[a]), dass bei der Darstellung einer Function durch eine andere φ derselben Gattung die Discriminante $\Delta_\varphi = \Pi(\varphi_\alpha - \varphi_\beta)^2$ als Nenner des darstellenden Ausdruckes eine Rolle spielt. Wir wollen eine weitere Eigenschaft der Discriminante herleiten.

Die Substitutionen der n Elemente z ordnen wir wie früher in eine Tabelle derart ein, dass die erste Zeile die Gruppe G der Function φ und jede der folgenden Zeilen je einen der Gruppe G conjugen Complex (§ 541) enthält:

$$\begin{array}{llllll} s_1 = 1, & s_2, & s_3, & \cdots & s_r; & G, \\ \sigma_2, & s_2\sigma_2, & s_3\sigma_2, & \cdots & s_r\sigma_2; & G\sigma_2, \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \sigma_\varrho, & s_2\sigma_\varrho, & s_3\sigma_\varrho, & \cdots & s_r\sigma_\varrho; & G\sigma_\varrho. \end{array} \qquad (r\varrho = n!)$$

Kommt eine Transposition etwa $(z_\alpha z_\beta)$ in einem der conjugen Complexe vor, z. B. in der zweiten Zeile, so zeigt dies an, dass φ_1 durch $(z_\alpha z_\beta)$ in φ_2 übergeführt wird. Es ist deswegen, wenn die Relation $z_\alpha = z_\beta$ herrscht, auch $\varphi_1 = \varphi_2$; denn bei der Gleichheit dieser Elemente wird ihre Umstellung ja keine Werthänderung in φ hervorrufen; und demgemäss ist ihre Differenz $(\varphi_1 - \varphi_2)$ durch $(z_\alpha - z_\beta)$ theibar.

Giebt es daher in der ersten Zeile, d. h. in der Gruppe G der Function φ selbst q Transpositionen der z, so kommen, weil das Schema alle Substitutionen und jede nur einmal enthält, die übrigen

$$\frac{1}{2}n(n-1) - q$$

Transpositionen der $z_1, z_2, \cdots z_n$ in den weiteren conjugen Complexen vor, und demnach werden auch $\frac{1}{2}n(n-1) - q$ Differenzen $(z_\alpha - z_\beta)$ bestehen, welche das Product

$$(21) \qquad (\varphi_1 - \varphi_2)(\varphi_1 - \varphi_3)\cdots(\varphi_1 - \varphi_\varrho)$$

theilen. Diese Differenzen der Form $(z_\alpha - z_\beta)$ sind alle unter einander verschieden, und somit ist (21) durch ihr Product theilbar.

Da die Gruppe $\sigma_2^{-1}G\sigma_2$, welche zu φ_2 gehört, dieselbe Constitution wie G besitzt, so ist auch das entsprechende Product

$$(21^a) \qquad (\varphi_2 - \varphi_1)(\varphi_2 - \varphi_3)\cdots(\varphi_2 - \varphi_\varrho)$$

durch $\frac{n(n-1)}{2} - q$ Transpositionen theilbar und die Discriminante

$$\Delta_\varphi = (-1)^{\frac{\varrho(\varrho-1)}{2}} \prod (\varphi_\lambda - \varphi_\mu) \qquad (\lambda < \mu;\ \lambda, \mu = 1, 2, \cdots \varrho)$$

durch das Product von $\varrho\left[\frac{n(n-1)}{2} - q\right]$ Differenzen von der Form $(z_\alpha - z_\beta)$.

Δ_φ ist symmetrisch in den z; das Vorkommen eines $(z_\alpha - z_\beta)$ beweist daher die Theilbarkeit durch die Discriminante der z, die wir mit Δ bezeichnen wollen; und da diese von der Dimension $n(n-1)$ ist, so erkennt man, dass die Discriminante jeder Function φ der Gattung G mindestens durch die Potenz

$$\Delta^{\varrho\left[\frac{1}{2} - \frac{q}{n(n-1)}\right]} \tag{22}$$

theilbar ist. Diese Potenz ist der grösste gemeinsame Theiler der Discriminanten der Functionen der Gattung. Die Richtigkeit dieser letzten Behauptung muss noch nachgewiesen werden.

Wir haben (§ 539) gezeigt, dass, falls nur $z_1, z_2, \cdots z_n$ von einander verschieden sind, bei sonst willkürlichen aber durch algebraische Gleichungen ausgedrückten Beziehungen der z unter einander stets zu G gehörige Functionen gefunden werden können, deren conjuge Werthe von einander verschieden sind, deren Discriminante also nicht gleich Null ist. Hätten nun die Discriminanten aller Functionen der Gattung G einen gemeinsamen Theiler $\omega(z_1, z_2, \cdots z_n)$, so würde es ausreichen, die z der Gleichung $\omega(z_1, \cdots z_n) = 0$ entsprechend zu wählen, um eine Gattung von lauter Functionen mit verschwindenden Discriminanten zu haben. Das ist aber, wie oben gezeigt wurde, nur bei Gleichheiten $z_\alpha = z_\beta$ möglich. Gemeinsame Theiler aller Discriminanten können demnach nur Potenzen der Theiler von Δ sein.

Es ist daher nur noch zu zeigen, dass die durch (22) bestimmte Potenz die höchste ist, welche als Theiler aller Discriminanten der Functionen einer Gattung heraustritt.

Wir bilden zu diesem Zwecke eine zu G gehörige Function (§ 539; 5[a])

$$\varphi_1 = \sum_{(k)} z_1^{k_1} z_2^{k_2} z_3^{k_3} \cdots z_n^{k_n}$$

und ihre Conjuge

$$\varphi_2 = \sum_{(l)} z_1^{l_1} z_2^{l_2} z_3^{l_3} \cdots z_n^{l_n},$$

wobei die k gemäss § 539 so angenommen sind, dass alle möglichen $n!$ Producte $z_1^{k_1} \cdots z_n^{k_n}$ unter einander verschieden werden, und wobei die l eine Permutation der k darstellen. Gesetzt nun $(\varphi_1 - \varphi_2)$ hätte den Factor $(z_1 - z_2)$, dann müssten bei der hinlänglich grossen Willkür in der Wahl der k die Functionen φ_1 und φ_2 aus Aggregaten von je zwei Gliedern sich zusammensetzen

$$z_1^{k_1} z_2^{k_2} z_3^{k_3} \cdots z_n^{k_n} \quad \text{und} \quad z_1^{k_2} z_2^{k_1} z_3^{k_3} \cdots z_n^{k_n},$$

die sich einander zuordnen und deren Differenz durch $(z_1 - z_2)$ und zwar nur durch diese erste Potenz theilbar ist. Bei solcher Zuordnung

ist es aber klar, dass φ_2 aus φ_1 durch die Transposition $\sigma = (z_1 z_2)$ entsteht; d. h. bei diesen Functionen kommt nur unter den am Anfange des Paragraphen vorausgesetzten Verhältnissen der Factor $(z_1 - z_2)$ und auch in keiner höheren als in der ersten Potenz vor.

Damit ist die Berechtigung erwiesen, (22) als Gattungsdiscriminante zu bezeichnen, d. h. als gemeinsamen Theiler der Discriminanten aller zur Gattung gehörigen Functionen. —

Ist G' eine unter G enthaltene Gattung, r' die Ordnung von G', $\varrho' = n! : r'$ ferner q' die Zahl der Transpositionen in G' und $r' = r\varkappa$, dann wird der Exponent $\varrho'\left[\frac{1}{2} - \frac{q'}{n(n-1)}\right] = \frac{\varrho}{\varkappa}\left[\frac{1}{2} - \frac{q'}{n(n-1)}\right]$ offenbar kleiner als $\varrho\left[\frac{1}{2} - \frac{q}{n(n-1)}\right]$, da $\varkappa$ mindestens $= 2$, und $q' \geqq q$ ist. Ist G' unter der Gattung G enthalten, dann theilt die Gattungsdiscriminante von G' diejenige von G*).

Die oben definirte Zahl q wird nur dann zu Null, wenn G keine Transpositionen besitzt; also stets dann, wenn die alternirende Gattung unter G enthalten ist. Natürlich ist dies aber nur eine hinreichende und keine nothwendige Bedingung.

Der Exponent in (22) verschwindet nur dann, wenn $q = \frac{1}{2} n(n-1)$ ist, d. h. wenn G die symmetrische Gattung repräsentirt und also conjuge Gattungen nicht vorhanden sind.

Aus (22) ist endlich ersichtlich, dass man die Gattungsdiscriminante jeder Gattung, ausgenommen die symmetrische, in eine solche Potenz erheben kann, dass die Gattungsdiscriminante einer beliebigen anderen Gattung sie theilt; oder mit anderen Worten, dass die irreductiblen Theiler aller Gattungsdiscriminanten, von der symmetrischen abgesehen, mit einander übereinstimmen.

Sechsundfünfzigste Vorlesung.

Composition und Isomorphismus.

§ 549. Wir haben bei der Behandlung von Abel'schen Gruppen (§ 509) den Begriff der vertauschbaren Elemente eingeführt, für welche also $\Theta_1 \Theta_2 = \Theta_2 \Theta_1$ wird. Diesem ordnet sich der Begriff der vertauschbaren Substitutionen unter; s und t heissen vertauschbar,

---

*) Kronecker, Grundzüge u. s. w. § 9. — Vgl. auch meinen Aufsatz: Journ. f. Math. 90, p. 164.

wenn das Resultat ihrer Composition von ihrer Stellung unabhängig ist, d. h. s und t sind vertauschbar, wenn

$$(1) \qquad st = ts, \quad \text{also} \quad s^{-1}ts = t \quad \text{und} \quad t^{-1}st = s$$

wird. Eine Substitution ändert sich nicht, wenn man sie durch eine mit ihr vertauschbare Substitution transformirt.

Potenzen einer und derselben Substitution sind miteinander vertauschbar.

Sind s und t miteinander vertauschbar, dann sind auch alle Potenzen s^λ von s mit allen t^μ von t vertauschbar. Es ist deshalb auch t^{-1} mit s vertauschbar, wenn t es ist, und es wird $tst^{-1} = s$.

Substitutionen, die kein Element mit einander gemeinsam haben, sind miteinander vertauschbar.

Alle Substitutionen, die mit einer gegebenen Substitution vertauschbar sind, bilden eine Gruppe. Denn aus den beiden Gleichungen

$$s^{-1}us = u \quad \text{und} \quad t^{-1}ut = u$$

folgt die den Satz beweisende dritte Gleichung (vgl. S. 258, Z. 12)

$$(st)^{-1}u(st) = t^{-1}[s^{-1}us]t = t^{-1}ut = u.$$

Alle Substitutionen einer Gruppe, die mit den Substitutionen einer anderen Gruppe vertauschbar sind, bilden aus gleichen Gründen auch eine Gruppe.

Sind die Substitutionen s und t miteinander vertauschbar, hat s die Ordnung n, und ist t^m die niedrigste Potenz von t, welche zugleich eine Potenz von s ist, so wird m entweder gleich der Ordnung von t oder gleich einem Theiler dieser Ordnung, wie leicht zu sehen ist. Dann lassen sich die sämmtlichen Substitutionen der Gruppe G geringsten Umfanges, welche s und t umfasst, eindeutig in der Form

$$(2) \qquad s^\alpha t^\beta \qquad (\alpha = 0, 1, \cdots n-1; \ \beta = 0, 1, \cdots m-1)$$

darstellen. Die Gruppe G hat also die Ordnung $m \cdot n$.

Zunächst ist es klar, dass jede Substitution von G als Combination von Potenzen des s und des t die Gestalt eines Potenzproductes mit beliebiger Factorenzahl

$$s^{\mu_1}t^{\nu_1}s^{\mu_2}t^{\nu_2}s^{\mu_3}t^{\nu_3} \dots s^{\mu_\varkappa}t^{\nu_\varkappa}$$

auftritt, wo die μ_α die Ordnung von s, und die ν_α die Ordnung von t nicht überschreiten können. Da nun s und t miteinander vertauschbar sind, kann man jedes solche Product

$$= s^{\mu_1+\mu_2+\cdots+\mu_\varkappa} \cdot t^{\nu_1+\nu_2+\cdots+\nu_\varkappa} = s^\mu t^\nu$$

setzen, wo auch μ und ν die Ordnungen der Substitutionen s und t nicht übertreffen. Da endlich t^m eine Potenz von s wird, so kann man die durch (2) gegebene Form dafür einsetzen.

Jede Substitution von G hat also die Form (2). Ferner sind alle (2) von einander verschieden. Denn wenn $b > \beta$ und $b, \beta < m$ sind, dann folgt aus

$$s^a t^b = s^\alpha t^\beta \quad \text{sofort} \quad s^{\alpha - a} = t^{b-\beta};$$

das aber führt zu dem Widerspruche mit der Voraussetzung, weil nun eine niedrigere Potenz von t als die m^{te} unter den Potenzen von s auftritt.

Als Corollar können wir aus diesem Satze entnehmen: Hat t die Ordnung n_1, und ist s^{m_1} die niedrigste Potenz von s, welche zugleich eine Potenz von t ist, so folgt für die Ordnung von G ebenso $m_1 \cdot n_1$. Folglich ist

$$m : m_1 = n_1 : n.$$

§ 550. Eine Gruppe

$$G = [1, s_2, s_3, \cdots s_r]$$

heisst mit einer Substitution t vertauschbar, wenn für jedes α eine Gleichung

$$(3) \qquad s_\alpha t = t s_\beta \quad \text{oder} \quad t^{-1} s_\alpha t = s_\beta$$

besteht, d. h. wenn man zu jedem α ein β finden kann, so dass (3) befriedigt wird.

Jede Substitution s_α von G wird hierbei durch t in eine nicht nothwendig wieder mit s_α zusammenfallende Substitution von G transformirt. Wir schreiben dies symbolisch

$$(3^a) \qquad t^{-1} G t = G,$$

wobei also links und rechts G nur als Inbegriff aller Substitutionen s_α auftritt.

Alle Substitutionen, die mit einer gegebenen Gruppe vertauschbar sind, bilden selbst eine Gruppe.

Ist G mit t vertauschbar, bedeudet r die Ordnung von G, ist ferner t^m die niedrigste Potenz von t, welche in G vorkommt, dann ist m gleich der Ordnung von t oder gleich einem Theiler dieser Ordnung. Es lassen sich nun sämmtliche Substitutionen der Gruppe H, die zugleich t und alle Substitutionen von G umfasst, in der Form

$$G t^\beta \qquad (\beta = 0, 1, \cdots m - 1)$$

darstellen, so dass diese Gruppe H also die Ordnung mr besitzt. Der Beweis dieses Satzes entspricht durchaus dem im vorigen Paragraphen bei dem specielleren Satze gegebenen.

§ 551. Zwei Gruppen

$$G = [1, s_2, s_3, \cdots s_r] \quad \text{und} \quad H = [1, t_2, t_3, \cdots t_q]$$

seien gegeben. Die angewendete Bezeichnung bedeutet, dass G von der Ordnung r ist und aus den Substitutionen $1, s_2, \cdots s_r$ besteht; und Aehnliches gilt für H (vgl. § 514).

Wir nennen G und H mit einander vertauschbar, wenn zu allen Indicespaaren α, β passende Indicespaare γ, δ gefunden werden können, welche die Gleichung

$$s_\alpha t_\beta = t_\gamma s_\delta \tag{4}$$

befriedigen. Wir drücken dies symbolisch durch die Formel aus

$$GH = HG. \tag{4*}$$

Eine Gruppe ist mit jedem ihrer Theiler vertauschbar.

Nun möge K die Gruppe aller Substitutionen sein, welche G und H gemein haben; dass diese Gesammtheit wirklich eine Gruppe bildet, erkennt man sofort. Es möge ferner G aus den conjugen Complexen (§ 538)

$$K;\ K\sigma_2;\ K\sigma_3;\ \cdots\ K\sigma_m,$$

und H aus den conjugen Complexen

$$K;\ K\tau_2;\ K\tau_3;\ \cdots\ K\tau_n$$

bestehen. Ist die Ordnung von K gleich r, so ist diejenige von G gleich rm, und diejenige von H gleich rn. Kein σ_α kann einem τ_β gleich werden.

Wir suchen diejenige Gruppe J geringsten Umfanges auf, welche alle Substitutionen von G und von H in sich fasst. Diese kann das kleinste gemeinsame Vielfache von G und H genannt werden, ebenso wie K als der grösste gemeinsame Theiler von G und H bezeichnet werden darf.

Jede Substitution der Gruppe J hat die Form eines Potenzproductes

$$s_\alpha^a\, t_\beta^b\, s_\gamma^c\, t_\delta^d \cdots;$$

dies kann wegen (4) auf die einfachere Form $s_\mu t_\nu$ gebracht werden. Nun gehört aber jedes t_ν zu einem Complexe $K\tau_\omega$, so dass man

$$s_\mu t_\nu = G(K\tau_\omega) = (GK)\tau_\omega = G\tau_\omega = K\sigma_v\tau_\omega$$

setzen kann, weil ja GK nichts anderes ist, als G selbst. Hieraus ist ersichtlich, dass die Ordnung von J nicht grösser als rmn sein kann.

Sie ist aber wirklich so gross. Denn wenn man $v = 1, 2, \cdots r$; $\omega = 1, 2, \cdots n$ setzt, erhält man lauter verschiedene Substitutionen.

Wäre nämlich

$$K\sigma_v\tau_\omega = K\sigma_w\tau_q \qquad (v, w \geqq mr;\ \omega, q \leqq n),$$

so würde

$$\tau_\omega\tau_q^{-1} = \sigma_v^{-1}K\sigma_w$$

folgen, d. h. eine Substitution von H gehörte der Gruppe G an; das ist aber nur möglich, wenn $q = \omega$ und $w = v$ ist.

Ist K der grösste gemeinsame Theiler, J das kleinste gemeinsame Vielfache der beiden vertauschbaren Gruppen G und H, und sind r, rm, rn die Ordnungen von K, G und H, so ist rmn die Ordnung von J.

§ 552. Ist eine Gruppe

$$G = [1, s_2, s_3, \cdots s_r]$$

gegeben, und ist H ein Theiler von G, derart dass H mit allen Substitutionen von G vertauschbar ist,

$$s_\alpha^{-1}Hs_\alpha = H \qquad (\alpha = 1, 2, \cdots r),$$

so müssen die conjugen Gruppen von H, welche Theiler von G sind, gleich H selbst werden. Für dieses Verhältnis von H zu G sind mancherlei Bezeichnungen eingeführt. H heisst nach F. Klein ein „ausgezeichneter" Theiler von G; nach G. Frobenius ein „monotypischer"; nach H. Weber ein „Normal"-Theiler; englische Autoren bezeichnen ein solches H als „selbst-conjugirt". Diese letzte Benennung ist wohl die treffendste; die Mängel, die man in ihr finden könnte, beruhen darin, dass sie nicht kurz genug ist; Bildungen wie „selbstconjugirte Maximaluntergruppe" wirken schleppend. Ich möchte deshalb im Anschluss an die bereits von mir benutzte Abkürzung „conjug" eine solche Gruppe einen autojugen Theiler von G nennen.

Hat eine Gruppe G einen von der Einheit verschiedenen autojugen Theiler niederer Ordnung, so heisst G zusammengesetzt; im entgegengesetzten Falle heisst es einfach.

Aus den Untersuchungen der vorigen Vorlesung können wir entnehmen, dass die symmetrische Gruppe zusammengesetzt und die alternirende A ein autojuger Theiler ist, da für jede Substitution s die Gleichung $s^{-1}As = A$ gilt.

Ferner ist die alternirende Gruppe, falls die Anzahl der Elemente > 4 wird, einfach. Denn dies ist genau der in § 543 behandelte Fall, da die dort benutzten σ sämmtlich zu A gehörten.

§ 553. Aus § 533, (16) entnehmen wir ferner, dass die lineare Gruppe U der

$$u = | h_\alpha \quad a_{\alpha 1} h_1 + a_{\alpha 2} h_2 + \cdots + a_{\alpha \nu} h_\nu + d_\alpha |$$
$$(\alpha = 1, 2, \cdots \nu;\ h_\alpha = 0, 1, \cdots n-1)$$

zusammengesetzt, und dass die cyklische Gruppe S der Substitutionen

$$s = | h_\alpha \quad h_\alpha + d_\alpha | \qquad (\alpha = 1, 2, \cdots \nu;\ h_\alpha = 0, 1, \cdots n-1)$$

ein autojuger Theiler von U ist.

Wir sind jetzt im Stande, die neu gewonnenen Begriffe dazu zu verwenden, um alle Substitutionen τ aufzufinden, welche der Gleichung

$$\tau^{-1} S \tau = S \tag{5}$$

genügen, also umgekehrt die grösste Gruppe zu bestimmen, für welche die cyklische Gruppe S ein autojuger Theiler ist.

Für die Behandlung dieses Problems brauchen wir den Hülfssatz: Jede beliebige Umwandlung der Indices $h_1, h_2, \cdots h_\nu$ lässt sich bei passender Wahl der ganzen Functionen $\varphi_1, \varphi_2, \cdots \varphi_\nu$ durch eine Substitution

$$| h_\alpha \quad \varphi_\alpha(h_1, h_2, \cdots h_\nu) | \tag{6}$$

ausdrücken. Um dies zu zeigen, lassen wir alle einzelnen $h_1, h_2, \cdots h_\nu$ die Werthreihe $0, 1, \cdots (n-1)$ unabhängig von einander durchlaufen; dann entspricht jedem Werthsysteme der h ein einziger Werth der Grösse

$$t = h_1 + n h_2 + n^2 h_3 + \cdots + n^{\nu-1} h_\nu, \tag{7}$$

und diese Werthe von t durchlaufen die ganze Zahlenreihe von 0 bis $(n^\nu - 1)$. Umgekehrt entspricht jedem dieser Werthe von t nur ein und stets ein System der h. Die Umformung eines Systems $h_1, h_2, \cdots h_\nu$ durch eine Substitution in das System $h'_1, h'_2, \cdots h'_\nu$ kann also auch so aufgefasst werden, dass dem Zahlenwerthe (7) ν Functionen $\psi_1(t)$, $\psi_2(t), \cdots \psi_\nu(t)$ zugeordnet werden, deren Werthe durch $h'_1, h'_2, \cdots h'_\nu$ bestimmt sind. Die $\psi_1, \psi_2, \cdots$ sind dabei durch die Lagrange'sche Interpolationsformel bestimmbar, und gemäss (7) kann endlich $\psi_\alpha(t) = \varphi_\alpha(h_1, h_2, \cdots h_\nu)$ gesetzt werden. —

Nachdem dieser Hülfssatz bewiesen ist, nehmen wir eine noch unbestimmte Substitution, in der die φ_α auch die Indices h liefern,

$$\tau = | h_\alpha \quad \varphi_\alpha(h_1, h_2, \cdots h_\nu) | \qquad (\alpha = 1, 2, \cdots \nu;\ h_\alpha = 0, 1, \cdots n-1)$$

und fragen, wie die Functionen φ_α beschaffen sein müssen, damit alle Ausdrücke

$$
(8)\quad
\begin{array}{l}
\tau^{-1}\cdot\left|\begin{matrix} h_1, h_2, \cdots h_\nu & h_1+1, h_2, \cdots h_\nu \end{matrix}\right|\cdot\tau,\\
\tau^{-1}\cdot\left|\begin{matrix} h_1, h_2, \cdots h_\nu & h_1, h_2+1, \cdots h_\nu \end{matrix}\right|\cdot\tau,\\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
\tau^{-1}\cdot\left|\begin{matrix} h_1, h_2, \cdots h_\nu & h_1, h_2, \cdots h_\nu+1 \end{matrix}\right|\cdot\tau
\end{array}
$$

zu arithmetischen Substitutionen werden. Durch diese Forderung ist nämlich nach § 524, (12) auch die anfängliche allgemeinere erfüllt.

Durch τ^{-1} geht jedes $\varphi_\alpha(h_1, \cdots h_\nu)$ in h_α über; durch $|h_1, h_2, \cdots h_1+1, h_2, \cdots|$ geht dann h_1 in h_1+1 über, während die folgenden h ungeändert bleiben; durch τ endlich geht (h_1+1) in $\varphi_\alpha(h_1+1, h_2, \cdots)$ über, u. s. f. Die erste Zeile von (8) ruft also folgende Aenderungen hervor: Jedes $\varphi_\alpha(h_1, h_2, \cdots h_\nu)$ geht in $\varphi_\alpha(h_1+1, h_2, \cdots h_\nu)$ über. Ebenso ruft die zweite Zeile von (8) die Umwandelung jedes $\varphi_\alpha(h_1, h_2, \cdots h_\nu)$ in $\varphi_\alpha(h_1, h_2+1, \cdots h_\nu)$ hervor u. s. w.

Sollen die so bestimmten Substitutionen sämmtlich arithmetische Substitutionen bedeuten, dann wird jeder durch ein $\varphi_\alpha(h_1, \cdots)$ dargestellte Index um eine Constante wachsen, und es muss also, wenn die $a_{\alpha 1}, a_{\alpha 2}, \cdots$ Constanten bedeuten,

$$
\begin{array}{l}
\varphi_\alpha(h_1+1, h_2, \cdots h_\nu) = \varphi_\alpha(h_1, h_2, \cdots h_\nu) + a_{\alpha 1},\\
\varphi_\alpha(h_1, h_2+1, \cdots h_\nu) = \varphi_\alpha(h_1, h_2, \cdots h_\nu) + a_{\alpha 2},\\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
\varphi_\alpha(h_1, h_2, \cdots h_\nu+1) = \varphi_\alpha(h_1, h_2, \cdots h_\nu) + a_{\alpha\nu}
\end{array}
$$

sein. Setzt man endlich $\varphi_\alpha(0, 0, \cdots 0) = d_\alpha$, so folgt, wenn man die eben erhaltenen Gleichungen dazu verwendet, um in $\varphi_\alpha(h_1, h_2, \cdots h_\nu)$ die Argumente der Reihe nach bis auf 0 zu verringern,

$$\varphi_\alpha(h_1, h_2, \cdots h_\nu) = a_{\alpha 1}h_1 + a_{\alpha 2}h_2 + \cdots + a_{\alpha\nu}h_\nu + d_\alpha.$$

Damit ist bewiesen: Die Substitutionen der linearen Gruppe U sind die einzigen, welche die cyklische Gruppe S in sich selbst transformiren. Jede Gruppe, für welche die cyklische Gruppe S ein autojuger Theiler wird, ist in der linearen Gruppe U enthalten.

§ 554. Wir leiten nun einige Hauptsätze über autojuge Theiler ab.

I) Ist H ein autojuger Theiler von G, und ist K ein beliebiger Theiler von G, dann sind H und K vertauschbar. Denn bezeichnen wir die Substitutionen von K mit $u_1, u_2, u_3, \cdots$, so wird für jedes α

$$u_\alpha^{-1} H u_\alpha = H.$$

II) Sind H und H autojuge Theiler von $G = [1, s_2, s_3, \cdots]$, dann ist die Gruppe geringsten Umfanges, welche H und H

enthält, auch ein autojuger Theiler von G; dieser kann freilich auch mit G zusammenfallen. Denn man hat

$$s_\alpha^{-1} H \mathsf{H} s_\alpha = \left(s_\alpha^{-1} H s_\alpha\right)\left(s_\alpha^{-1} \mathsf{H} s_\alpha\right) = H\mathsf{H},$$

und daraus folgt der Satz sofort.

III) Sind H und H autojuge Theiler von $G = [1, s_2, s_3, \cdots]$, dann ist der grösste gemeinsame Theiler $\mathfrak{H}$ von H und H auch ein autojuger Theiler von G. Denn man hat die Reihe der Gleichungen

$s_\alpha^{-1} \mathfrak{H} s_\alpha = H$, weil $\mathfrak{H}$ zu H gehört; und

$s_\alpha^{-1} \mathfrak{H} s_\alpha = \mathsf{H}$, „ $\mathfrak{H}$ „ H „ ; folglich ist

$s_\alpha^{-1} \mathfrak{H} s_\alpha = \mathfrak{H}$, weil es zu H und zu H gehört.

IV) Sind $H = [1, t_2, t_3, \cdots]$ und $\mathsf{H} = [1, \tau_2, \tau_3, \cdots]$ zwei autojuge Theiler von G; ist ferner der grösste gemeinsame Theiler $\mathfrak{H}$ von H und H gleich $[1, \mathrm{t}_2, \mathrm{t}_3, \cdots]$, und ist $K = [1, u_2, u_3, \cdots]$ irgend eine in H enthaltene und $\mathfrak{H}$ enthaltende Gruppe, dann ist K mit allen Substitutionen von H vertauschbar. Denn es ist

$$\tau_\alpha^{-1} u_\beta^{-1} \tau_\alpha u_\beta = \left(\tau_\alpha^{-1} u_\beta^{-1} \tau_\alpha\right) u_\beta = t_\gamma u_\beta = t_\delta,$$

weil u_β^{-1} zu H gehört und H mit H vertauschbar ist; ferner ist aber zugleich auch

$$\tau_\alpha^{-1} u_\beta^{-1} \tau_\alpha u_\beta = \tau_\alpha^{-1}\left(u_\beta^{-1} \tau_\alpha u_\beta\right) = \tau_\alpha^{-1} \tau_\gamma = \tau_\varepsilon,$$

weil H autojug in G ist. Deshalb wird die linke Seite der beiden letzten Gleichungen zu $\mathfrak{H}$ gehören müssen, da sie gleichzeitig ein t und ein τ wird; d. h. man hat

$$\tau_\alpha^{-1} u_\beta^{-1} \tau_\alpha u_\beta = \mathrm{t}_\vartheta, \quad \tau_\alpha^{-1} u_\beta^{-1} \tau_\alpha = \mathrm{t}_\vartheta u_\beta^{-1};$$

da nun u_β^{-1} und t_ϑ der Gruppe K angehören, so ist endlich auch

$$\tau_\alpha^{-1} u_\mu \tau_\alpha = u_\nu; \quad \tau_\alpha^{-1} K \tau_\alpha = K.$$

Hierdurch ist der Beweis geliefert.

§ 555. Ist H ein autojuger Theiler von G, der so beschaffen sein soll, dass es keinen anderen autojugen Theiler von G giebt, welcher H in sich einschliesst, so nennen wir H einen autojugen Maximaltheiler von G.

Nun sei G irgend eine zusammengesetzte Gruppe, und die Reihe

$$G,\ G_1,\ G_2,\ \cdots\ G_\nu,\ 1 \tag{9}$$

möge so gewählt sein, dass jedes ihrer Glieder G_α $(\alpha \geqq 1)$ autojuger Maximaltheiler des vorhergehenden wird. Dann nennen wir (5) eine zu G gehörige Compositionsreihe. Die Ordnungen der einzelnen Gruppen in (5) bezeichnen wir entsprechend

$$r,\ r_1,\ r_2,\ \cdots\ r_\nu,\ 1;$$

jede dieser Zahlen ist ein Theiler der Vorhergehenden. Wir setzen ferner

$$\frac{r}{r_1} = e_1,\quad \frac{r_1}{r_2} = e_2,\ \cdots\ \frac{r_{\nu-1}}{r_\nu} = e_\nu,\quad \frac{r_\nu}{1} = e_{\nu+1};$$

dann nennen wir die Quotienten $e_1,\ e_2, \cdots e_\nu,\ e_{\nu+1}$ die zur Compositionsreihe (5) gehörigen Factoren oder die Compositionsfactoren.

Es kann vorkommen, dass eine Gruppe verschiedene autojuge Maximaltheiler besitzt. Infolge dessen kann es auch eintreten, dass zu einer Gruppe G verschiedene Compositionsreihen gehören. Wir werden nun beweisen, dass, wie auch die Reihen gewählt werden mögen, die einzelnen Compositionsfactoren, abgesehen von ihrer Aufeinanderfolge, für alle Reihen dieselben, und ihrer Gesammtheit nach daher invariant sind.

Es bilde neben (9) auch noch die Reihe von Gruppen

$$G,\ \Gamma_1,\ \Gamma_2,\ \cdots\ \Gamma_\mu,\ 1 \tag{9^a}$$

eine zu G gehörige Compositionsreihe mit den Ordnungen

$$r,\ \varrho_1,\ \varrho_2,\ \cdots\ \varrho_\mu,\ 1$$

und den Compositionsfactoren

$$\frac{r}{\varrho_1} = \eta_1,\quad \frac{\varrho_1}{\varrho_2} = \eta_2,\ \cdots\ \frac{\varrho_{\mu-1}}{\varrho_\mu} = \eta_\mu,\quad \frac{\varrho_\mu}{1} = \eta_{\mu+1}.$$

Wir können von vornherein annehmen, dass Γ_1 von G_1 verschieden sei, da ja im entgegengesetzten Falle die Anfangsglieder, welche dem zu beweisenden Satze schon entsprechen würden, einfach weggelassen werden könnten.

Die Gruppe geringsten Umfanges, welche Γ_1 und G_1 enthält, sei H; der grösste gemeinsame Theiler von Γ_1 und G_1 sei K, und k die Ordnung von K. Nach II) des vorigen Paragraphen ist H ein autojuger Theiler von G; da er aber die beiden Maximaltheiler G_1 und Γ_1 umfasst und eine höhere Ordnung besitzt als jeder derselben, so fällt H mit G zusammen, d. h. man hat $H = G$. Die Ordnung von H ist nach § 551 gleich $r_1 \cdot \frac{\varrho_1}{k}$; folglich hat man die Gleichungen

$$\frac{r_1 \varrho_1}{k} = r = r_1 e_1 = \varrho_1 \eta_1;$$

und deswegen

(10) $$\varrho_1 = k \cdot e_1, \quad r_1 = k \cdot \eta_1.$$

Nach. III) des vorigen Paragraphen ist K ein autojuger Theiler von G und also auch autojug in G_1 und in Γ_1.

Endlich ist K auch ein autojuger Maximaltheiler von G_1 und von Γ_1. Denn gäbe es zwischen G_1 und K noch einen in G_1 enthaltenen und K umschliessenden autojugen Theiler L, so wäre nach § 554, IV) L mit allen Substitutionen von Γ_1 vertauschbar. Da ferner L mit allen Substitutionen von G_1 vertauschbar ist, so findet dasselbe auch für die Substitutionen von $H = G$ statt, d. h. L ist sogar autojuger Theiler von G. Dann würde die Gruppe geringsten Umfanges, welche L und Γ_1 enthält, ein autojuger Theiler von G werden, ohne mit G zusammenzufallen; denn nach dem Lehrsatze aus § 551 wäre ihre Ordnung geringer als $r_1 \cdot \frac{\varrho_1}{k}$, d. h. geringer als r. Andrerseits würde sie die Gruppe Γ_1 enthalten; also könnte Γ_1 kein autojuger Maximaltheiler sein. Es darf sonach keine solche Gruppe L geben; d. h. K ist autojuger Maximaltheiler von G_1 und von Γ_1.

Man könnte demnach neben (5) und (5ª) noch zwei Compositionsreihen für G construiren, deren drei Anfangsglieder bezw.

(9ᵇ) $$G,\ G_1,\ K,\ \cdots \quad \text{und} \quad G,\ \Gamma_1,\ K,\ \cdots$$

und deren Anfangsfactoren gemäss (10)

$$e_1,\ \eta_1,\ \cdots \quad \text{und} \quad \eta_1,\ e_1,\ \cdots$$

sind. Da K in beiden Reihen auftritt, kann man in beiden die auf die Gruppe K folgenden Glieder identisch machen.

Der ausgesprochene Satz wird daher bewiesen sein, wenn er für (9) und die erste Reihe aus (9ᵇ) und ebenso für (9ª) und die zweite Reihe von (9ᵇ) gilt. Dadurch wird der Beweis aber auf Reihen reducirt, die schon in den Anfangsfactoren übereinstimmen.

Wendet man dieselben Schlüsse auf sie an, so erkennt man die Wahrheit des Satzes: Die Compositionsfactoren sind, abgesehen von ihrer Aufeinanderfolge, für alle zu G gehörigen Compositionsreihen dieselben. Daher ist auch die Anzahl der Gruppen dieser Reihen constant.

Die allmähliche Umwandlung der Gruppenreihe (9) in (9ª) führt im allgemeinen Falle bei ν Zwischengliedern zwischen G und 1 auf 2^ν Reihen. Im Falle $\nu = 4$ z. B. hat man Folgendes. Die Umwandlung erfolgt durch

1)	$G,\ G_1,\ G_2,\ G_3,\ G_4,\ 1$	9)	$G,\ \Gamma_1,\ J_2,\ J_3,\ J_4,\ 1$
2)	$G,\ G_1,\ G_2,\ G_3,\ L_4,\ 1$	10)	$G,\ \Gamma_1,\ J_2,\ J_3,\ N_4,\ 1$
3)	$G,\ G_1,\ G_2,\ K_3,\ L_4,\ 1$	11)	$G,\ \Gamma_1,\ J_2,\ P_3,\ N_4,\ 1$
4)	$G,\ G_1,\ G_2,\ K_3,\ K_4,\ 1$	12)	$G,\ \Gamma_1,\ J_2,\ P_3,\ P_4,\ 1$
5)	$G,\ G_1,\ J_2,\ K_3,\ K_4,\ 1$	13)	$G,\ \Gamma_1,\ \Gamma_2,\ P_3,\ P_4,\ 1$
6)	$G,\ G_1,\ J_2,\ K_3,\ M_4,\ 1$	14)	$G,\ \Gamma_1,\ \Gamma_2,\ P_3,\ Q_4,\ 1$
7)	$G,\ G_1,\ J_2,\ J_3,\ M_4,\ 1$	15)	$G,\ \Gamma_1,\ \Gamma_2,\ \Gamma_3,\ Q_4,\ 1$
8)	$G,\ G_1,\ J_2,\ J_3,\ J_4,\ 1$	16)	$G,\ \Gamma_1,\ \Gamma_2,\ \Gamma_3,\ \Gamma_4,\ 1.$

Hierbei sind die Reihen 1) und 16) die Ausgangspunkte. Zwischen sie schieben sich zunächst 8) und 9) ein, so dass man hat

1), 8); 9), 16);

dann zwischen 1) und 8) als neue Glieder 4) und 5); und zugleich zwischen 9) und 16) als neue 12) und 16), so dass entsteht

1), 4); 5), 8); 9), 12); 13), 16)

u. s. f. Bei dieser Tabelle findet also von jeder Nummer zur folgenden nur je eine Abänderung statt.

Nach der Einführung des Begriffes der Composition können wir den Satz aus § 545 unserer Theorie anfügen. Er heisst in der anzuwendenden Nomenclatur: Ist der zum Uebergange von G zu H gehörige Compositionsfactor gleich einer Primzahl p, dann gehört die p^{te} Potenz jeder zu G gehörigen, nicht in H vorkommenden Potenz zu dieser Gruppe H. Der Beweis hierfür ist in § 545 gegeben; er folgt daraus, dass wenn man eine Substitution σ aus G, die nicht zu H gehört, mit H verbindet, hieraus G entstehen muss, sowie daraus, dass $\sigma H = H\sigma$ ist.

Wir können hier noch hinzufügen, was dann als wesentliche Eigenschaft der Compositionsreihe auftritt, dass zwei Substitutionen s_α und s_β von G bis auf eine Substitution von H mit einander vertauschbar sind, falls der Compositionsfactor eine Primzahl ist. In der That können wir dann

$$s_\alpha = t_\alpha \sigma^\varrho, \quad s_\beta = t_\beta \sigma^\tau$$

setzen, wenn t_α und t_β zu H gehören. Daraus folgt

$$s_\alpha s_\beta = t_\alpha \sigma^\varrho \cdot t_\beta \sigma^\tau = t_\alpha (\sigma^\varrho t_\beta \sigma^{-\varrho}) \sigma^{\tau+\varrho} = t_\alpha t_\gamma \sigma^{\tau+\varrho} = t_\delta \sigma^{\tau+\varrho},$$
$$s_\beta s_\alpha = t_\beta \sigma^\tau \cdot t_\alpha \sigma^\varrho = t_\beta (\sigma^\tau t_\alpha \sigma^{-\tau}) \sigma^{\varrho+\tau} = t_\beta t_\varepsilon \sigma^{\tau+\varrho} = t_\vartheta \sigma^{\tau+\varrho},$$
$$s_\alpha s_\beta = s_\beta s_\alpha \cdot t_\mu,$$

und in der letzten Gleichung liegt der Beweis für die Behauptung.

Den letzten Lehrsatz können wir umkehren: Sind die Substitutionen s_α, s_β, $\cdots$ von G bis auf Substitutionen t von H mit einander vertauschbar, dann ist der zugehörige Compositionsfactor eine Primzahl.

Wählen wir ein σ aus G, welches nicht zu H gehört, und dessen $\varkappa^{\text{te}}$ Potenz ($\varkappa > 1$) die erste in H vorkommende ist, so wird die Gesammtheit der Substitutionen von

$$H, \; H\sigma, \; H\sigma^2, \; \cdots \; H\sigma^{\varkappa-1}$$

eine Gruppe bilden; denn es ist

$$H\sigma^\alpha = \sigma^\alpha H,$$

da wir ja H als autojugen Theiler von G angenommen haben. Diese Gruppe ist in G enthalten. Sie ist ferner autojug zu G. Denn man hat

$$s_\alpha^{-1} H\sigma^\beta s_\alpha = s_\alpha^{-1} H s_\alpha \cdot s_\alpha^{-1}\sigma^\beta s_\alpha = H \cdot s_\alpha^{-1}\sigma^\beta s_\alpha,$$

und weil die Substitutionen von G mit einander bis auf solche von H permutabel sind, so wird

$$s_\alpha^{-1} H\sigma^\beta s_\alpha = H \cdot t_\gamma \sigma^\beta s_\alpha^{-1} s_\alpha = H\sigma^\beta.$$

Demnach muss die aus allen Substitutionen von

$$H, \; H\sigma, \; H\sigma^2, \; \cdots \; H\sigma^{\varkappa-1}$$

bestehende Gruppe mit G zusammenfallen, weil G in der Compositionsreihe unmittelbar vor H steht.

Wäre nun $\varkappa$ keine Primzahl, und q ein Theiler von $\varkappa$, dann wäre

$$H, \; H\sigma^q, \; H\sigma^{2q}, \; \cdots$$

aus gleichen Gründen eine Gruppe, die in G enthalten ist, H enthält und autojug von G ist. Diese Gruppe würde also in die Reihe der Composition zwischen G und H eingeschoben werden müssen, was unseren Voraussetzungen widerspricht. Folglich ist $\varkappa$ eine Primzahl. Von dieser ergiebt sich sofort, dass sie der Compositionsfactor wird, der beim Uebergange von G zu H auftritt.

Die Gleichung $s_\alpha s_\beta = s_\beta s_\alpha \cdot t_\mu$ ist also charakteristisch dafür, dass der Compositionsfactor eine Primzahl ist.

§ 556. Im Allgemeinen wird ein jedes beliebige Glied der Compositionsreihe

$$(9) \qquad G, \; G_1, \; G_2, \; \cdots \; G_\nu, \; 1$$

nur vom vorhergehenden Gliede autojuger Theiler sein; es können aber auch Glieder auftreten, die autojug in weiter zurückliegenden Gruppen vorkommen. Insbesondere können gewisse Glieder G_a, G_b, $\cdots$ autojuge Theiler von G selbst sein.

Wählen wir aus der Reihe (9) nur diejenigen aus

$$(11) \qquad G, H, J, K, \cdots L, M, 1,$$

welche autojuge Theiler von G sind, so heisst die Reihe (11) die Hauptcompositionsreihe oder kürzer die Hauptreihe von G.

Gesetzt, die Hauptreihe stimmt nicht mit der Reihe der Zusammensetzung überein, dann mögen sich z. B. zwischen H und J noch andere Gruppen von (9) einschieben. Die erste auf H in (9) folgende sei H_1'; dann ist H_1' autojug in H, aber nicht in G. Transformiren wir nun H_1' durch alle Substitutionen von G, so mögen dabei q conjuge Gruppen entstehen, und zwar sei wenn $t_2, t_3, \cdots$ Substitutionen von G sind,

$$(12) \qquad t_2^{-1} H_1' t_2 = H_1'', \quad t_3^{-1} H_1' t_3 = H_1''', \quad \cdots \quad t_q^{-1} H_1' t_q = H_1^{(q)}.$$

Da

$$t_2^{-1} H t_2 = t_3^{-1} H t_3 = \cdots = t_q^{-1} H t_q = H,$$
$$t_2^{-1} J t_2 = t_3^{-1} J t_3 = \cdots = t_q^{-1} J t_q = J,$$

so ist jedes $H_1^{(\alpha)}$ Theiler von H und Multiplum von J.

Ferner ist jedes $H_1^{(\alpha)}$ autojug in H. Denn weil H autojug in G ist, so kann man für jedes u_λ in H ein u_μ in H so bestimmen, dass

$$t_\alpha u_\lambda t_\alpha^{-1} = u_\mu, \quad u_\mu t_\alpha = t_\alpha u_\lambda$$

wird; dann folgt aus $u_\mu^{-1} H_1' u_\mu = H_1'$

$$H_1^{(\alpha)} = t_\alpha^{-1} H_1' t_\alpha = t_\alpha^{-1} u_\mu^{-1} H_1' u_\mu t_\alpha = u_\lambda^{-1} t_\alpha^{-1} H_1' t_\alpha u_\lambda = u_\lambda^{-1} H_1^{(\alpha)} u_\lambda,$$

und diese Gleichung beweist die Behauptung.

Endlich ist $H_1^{(\alpha)}$ ein autojuger Maximaltheiler von H. Denn schöbe sich zwischen H und $H_1^{(\alpha)}$ noch ein $\Gamma^{(\alpha)}$ ein, welches autojug in H wäre, so würde durch Transformation mit t_α^{-1} daraus ein Γ' entstehen, welches umfassender wäre als H_1' und autojug in H.

Man kann also jetzt nach dem vorigen Paragraphen eine Compositionsreihe für G construiren, die vom Beginn bis zu H mit (9) übereinstimmt, dann $H_1^{(\alpha)}$ folgen lässt und, da dies J enthält, über J fortgeht, wie leicht zu sehen ist; diese kann man, wie gezeigt wurde, so einrichten, dass auf $H_1^{(\alpha)}$ der grösste gemeinsame Theiler von $H_1^{(\alpha)}$ und $H_1^{(\beta)}$ folgt; und zwar gilt dies für jedes Paar α, β. Diesen grössten gemeinsamen Theiler bezeichnen wir mit $H_2^{(\alpha\beta)}$.

Dann können wir von $H_2^{(\alpha\beta)}$, $H_2^{(\alpha\gamma)}$ ebenso zu ihrem grössten gemeinsamen Theiler $H_3^{(\alpha\beta\gamma)}$ übergehen, u. s. f. Dieses $H_3^{(\alpha\beta\gamma)}$ ist dann gleichzeitig der grösste gemeinsame Theiler von $H_1^{(\alpha)}$, $H_1^{(\beta)}$ und $H_1^{(\gamma)}$.

Da beim Fortschreiten jede der neuen Gruppen das J enthält, so kommt man nach q Schritten zu J als zum grössten gemeinsamen Theiler von $H_1', H_1'', \cdots H_1^{(q)}$.

Nun möge zum Uebergange von H zu H_1' der Compositionsfactor e gehören. Derselbe gehört dann zum Uebergange von H zu jedem $H_1^{(\alpha)}$ in (12), da alle diese Gruppen einander ähnlich sind. Folglich gehört nach dem vorigen Paragraphen zum Uebergange jedes $H_1^{(\alpha)}$ zu jedem $H_2^{(\alpha\beta)}$ wiederum der Factor e u. s. f. Es tritt also bei jeder Reihe

$$H, H_1, H_2, \cdots H_{q-1}, J$$

überall, d. h. q-mal der Factor e auf. Wenn man von G aus in dem Falle, dass Reihe und Hauptreihe nicht übereinstimmen, die eben getroffene Anordnung macht, indem man zwischen je zwei Gruppen der Hauptreihe H, J alle Gruppen der Reihe einschaltet, dann tritt der gleiche Compositionsfactor e für alle Zwischenglieder auf. Der zur Hauptreihe gehörige Compositionsfactor ist also eine Potenz von e.

Ist G keine einfache Gruppe, und besteht also (9) aus mehr als den beiden Gliedern G und 1, so hat G auch eine Hauptcompositionsreihe, da ja natürlich das erste auf G folgende Glied der Compositionsreihe in G selbst autojug ist.

Wenn in der Compositionsreihe

$$G, G_1, G_2, \cdots G_\varkappa, G_{\varkappa+1}, \cdots G_\nu, 1 \tag{9}$$

mit den Compositionsfactoren

$$e_1, e_2, \cdots e_\varkappa, e_{\varkappa+1}, \cdots e_\nu, e_{\nu+1}$$

das Glied $G_\varkappa$ der Hauptreihe angehört, und wenn unter $e_{\varkappa+1}, \cdots e_\nu, e_{\nu+1}$ verschiedene Zahlen vorkommen, dann liegt zwischen $G_\varkappa$ und 1 in (9) noch eine mit G autojuge Gruppe, d. h. noch ein Glied der Hauptreihe. Denn wäre keine der Gruppen $G_{\varkappa+1}, \cdots G_\nu$ zur Hauptreihe gehörig, dann wäre

$$e_{\varkappa+1} = e_{\varkappa+2} = \cdots = e_\nu = e_{\nu+1}. \text{ —}$$

Man sieht ferner leicht, dass wenn H ein autojuger Theiler von G ist, eine Compositionsreihe construirt werden kann, welche H als Glied enthält. —

Wir bemerken, dass auch hier verschiedene Hauptreihen möglich, aber die Producte der Factoren, welche dem Uebergange von jedem Gliede der Hauptreihe zum folgenden angehören, nicht invariant sind*).

*) W. Burnside, Theory of groups, Cambr. 1897, § 92 behauptet die Invarianz.

Dies zeigt das Beispiel:

$$G = [1, (z_1z_2), (z_3z_4), (z_1z_2)(z_3z_4), (z_1z_3)(z_2z_4), (z_1z_4)(z_2z_3), (z_1z_3z_2z_4), (z_1z_4z_2z_3)];$$

$$G_1 = [1, (z_1z_2)(z_3z_4), (z_1z_3)(z_2z_4), (z_1z_4)(z_2z_3)];$$

$$G_2 = [1, (z_1z_2)(z_3z_4)].$$

Hier fällt die Hauptreihe mit der Reihe $G, G_1, G_2, G_3 = 1$ zusammen. Gleichzeitig ist aber für

$$G_1' = [1, (z_1z_2), (z_3z_4), (z_1z_2)(z_3z_4)]; \quad G_2' = [1, (z_1z_2)]$$

auch $G, G_1', G_2', G_3' = 1$ eine Compositionsreihe, aus welcher $G, G_1', 1$ als Hauptreihe heraustritt. Im ersten Falle besitzt demnach die Hauptreihe vier Glieder, hier dagegen nur drei. —

Wir wollen die am Schluss von § 555 aufgestellten Theoreme über den Fall, dass ein Compositionsfactor eine Primzahl wird, hier verwenden.

Wenn in der Compositionsreihe von G die Glieder

$$\cdots H, H_1, H_2, \cdots H_{q-1}, J, \cdots$$

vorkommen, und H, J aufeinander folgende Glieder der Hauptreihe sind, wenn ferner zum Uebergange von H zu H_1 der Compositionsfactor p gehört, der eine Primzahl sein soll, so erinnern wir uns, dass auf H in der Compositionsreihe auch ausser $H_1 = H_1'$ noch Gruppen

$$H_1'', H_1''', \cdots H_1^{(q)}$$

folgen können, und dass J der grösste gemeinsame Theiler dieser Gruppen ist.

Nun waren die Substitutionen von H mit einander bis auf solche von H_1' vertauschbar; das Gleiche gilt für $H_1'', H_1''', \cdots$, d. h. die Substitutionen von H sind mit einander bis auf Substitutionen von J vertauschbar.

Umgekehrt, wenn dies stattfindet, so sind auch die Substitutionen von H_{q-1} unter einander bis auf die von J vertauschbar. Folglich gehört dazu als Compositionsfactor eine Primzahl p, und deshalb zum Uebergange von H zu J die Potenz p^q. Die Vertauschbarkeit der Substitutionen von H bis auf solche von J ist also charakteristisch dafür, dass als Factor der Compositionsreihe dabei eine Primzahl auftritt. Da auf die vorletzte Gruppe der Hauptreihe die Einheitsgruppe folgt, so muss diese Gruppe unter einander vertauschbare Substitutionen haben. Die vorletzte Gruppe der Hauptreihe ist eine Abel'sche Gruppe.

§ 557. Wir gehen auf eine andere wichtige Erscheinung ein, auf den Isomorphismus.

Es kommt vor, dass die Substitutionen zweier Substitutionengruppen G und Γ einander so zugeordnet werden können, dass auch dem Producte zweier willkürlichen Substitutionen von G das Product der zugeordneten Substitutionen von Γ zugeordnet ist. In diesem Falle heissen G und Γ isomorph.

Am einfachsten gestalten sich die Verhältnisse, wenn jeder Substitution der einen Gruppe nur eine der anderen zugeordnet ist. In diesem Falle sprechen wir von einstufigem Isomorphismus.

Jedem Theiler H von G entsprechen die Substitutionen eines Theilers H von Γ. Ist H autojug in G, dann ist H autojug in Γ; denn aus

$$G^{-1}HG = H \quad \text{folgt} \quad \Gamma^{-1}\mathsf{H}\Gamma = \mathsf{H}.$$

Ist H ein autojuger Maximaltheiler in G, dann gilt das Entsprechende für H in Γ. Denn aus der Existenz einer zwischen Γ und H tretenden autojugen Gruppe Λ würde die einer entsprechenden L in G folgen.

Der Compositionsreihe (und auch der Hauptcompositionsreihe) von G entspricht die aus der isomorphen Gruppe Γ abgeleitete entsprechende Folge von Gruppen als Reihe (bezw. als Hauptreihe).

Einstufig-isomorphe Gruppen besitzen gleiche Ordnungen, während ihre Grade verschieden sein können. Sie haben ferner gleiche Compositionsfactoren; sie sind gleichzeitig einfach oder zusammengesetzt.

So bleibt eine Reihe wichtiger Eigenschaften, die mit der Multiplication der Elemente zusammenhängen, bei isomorphen Gruppen invariant.

Es ergiebt sich hieraus, dass diejenigen Gruppeneigenschaften, welche allen isomorphen Gruppen gemeinsam sind, als in der Natur der Gruppe tiefer begründet angesehen werden können. So haben wir die Ordnung als Invariante einstufig-isomorpher Gruppen, den Grad hingegen nicht. Wie wir ferner soeben sahen, bleibt für isomorphe Gruppen die Eigenschaft, einfach oder zusammengesetzt zu sein, bestehen.

Wir wollen eine Methode angeben, zu einer vorgelegten Gruppe G der Ordnung r eine einstufig-isomorphe von besonders interessanten Eigenthümlichkeiten zu bilden. Es sei, wie in § 539, $\varphi(z_1, \cdots z_n) = \varphi_1$ eine Galois'sche Function, d. h. eine solche, die $n!$ Werthe besitzt. Wir wenden auf φ_1 die Substitutionen der Gruppe

$$G = [1, s_2, s_3, \cdots s_r]$$

an und erhalten daraus die Reihe der r verschiedenen Werthe

(12) $$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_r.$$

Wird nun auf diese Reihe ein s_α angewendet, dann geht die Gesammtheit ihrer Elemente in sich selber über. Wir bezeichnen die Umwandlung von $\varphi_\varkappa$ durch s_α mit $\varphi_{\alpha_\varkappa}$; dann ruft also s_α aus der Anordnung (12) hervor

$$\varphi_{\alpha_1}, \varphi_{\alpha_2}, \varphi_{\alpha_3}, \cdots \varphi_{\alpha_r}.$$

Wir setzen jetzt als Zeichen für diesen Uebergang

$$\sigma_\alpha = \begin{pmatrix} \varphi_\varkappa \\ \varphi_{\alpha_\varkappa} \end{pmatrix} \qquad (\varkappa = 1, 2, \cdots r),$$

dann wird die Wirkung von s_α auf die Elemente (12) als Functionen der z aufgefasst dieselbe sein, wie die von σ_α auf dieselben als beliebige Elemente aufgefassten Glieder; folglich wird, wenn sich auch s_β und σ_β entsprechen, die Wirkung von $s_\alpha \cdot s_\beta$ dieselbe sein, wie die von $\sigma_\alpha \cdot \sigma_\beta$, d. h. auch $s_\alpha s_\beta$ und $\sigma_\alpha \sigma_\beta$ entsprechen einander; wir haben demnach Isomorphismus zwischen den s und den σ.

Es können bei dieser Zuordnung nicht zwei verschiedene $s_\varkappa$ und s_λ das gleiche $\sigma_\varkappa = \sigma_\lambda$ hervorrufen. Denn sonst würden sich $s_\varkappa s_\lambda^{-1}$ und $\sigma_\varkappa \sigma_\lambda^{-1} = 1$ entsprechen, d. h. die von 1 verschiedene Substitution $s_\varkappa s_\lambda^{-1}$ riefe keine Umänderung bei (12) hervor, während doch sogar jedes Element von (12) sich durch jede Substitution ändert. Umgekehrt entspricht jedem $s_\varkappa$ ein $\sigma_\varkappa$. Folglich findet einstufiger Isomorphismus zwischen den s und den σ statt, wobei die σ eine Gruppe Γ von der Ordnung r bilden.

Γ ist auch vom Grade r, da seine Elemente $\varphi_1, \varphi_2, \cdots \varphi_r$ sind. Γ ist so beschaffen, dass jede seiner Substitutionen σ (abgesehen von $\sigma_1 = 1$) alle Elemente umsetzt; denn jedes φ ist eine $n!$-werthige Function. Jedes σ ist regulär, d. h. es enthält nur Cyklen von gleich vielen Elementen; denn wäre dies nicht der Fall, dann würde eine passende Potenz, ohne $= 1$ zu sein, einige Elemente nicht umstellen. —

Wir können die angegebene Methode dadurch abändern, dass wir für φ eine beliebige q-werthige Function ($q > 2$) mit den Werthen

(12ᵃ) $$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_q$$

nehmen und auf diese Reihe die Substitutionen s_α der Gruppe G anwenden, um dadurch jedem s_α ein σ zuordnen zu können. Ebenso wie oben folgt dann, dass dem Producte $s_\alpha s_\beta$ das Product $\sigma_\alpha \sigma_\beta$ entspricht, und aus § 543 entnehmen wir, dass jedem s_α nur Ein σ_α

entspricht, weil sonst ein s bestehen müsste, welches von der Einheit verschieden ist und doch alle Elemente aus (12[a]) ungeändert lässt. Die neue Gruppe Γ ist sonach einstufig-isomorph zu G; aber freilich fehlen ihr die weiteren Eigenschaften der oben abgeleiteten Gruppe, die der Benutzung einer Galois'schen Function entstammte.

§ 558. Wir hatten zu Beginn des vorigen Paragraphen den Begriff des Isomorphismus weiter gefasst, indem wir nur forderten, dass eine Zuordnung der Substitutionen von G und Γ möglich sein solle, bei welcher aus dem Entsprechen von s_α und σ_α und demjenigen von s_β und σ_β auch das von $s_\alpha s_\beta$ und $\sigma_\alpha \sigma_\beta$ für alle α, β folgt. Hierbei können einem s mehrere σ und zugleich einem σ mehrere s entsprechen. Auf diesen allgemeinsten Fall wollen wir jedoch nicht eingehen, sondern uns allein mit demjenigen beschäftigen, in welchem der einen Substitution 1 von Γ in G eine Reihe von m Substitutionen $s_1', s_2', \cdots s_m'$ entspricht, und umgekehrt jeder von diesen m Substitutionen s' allein 1 aus Γ. Dann sagen wir, G stehe zu Γ in m-ein-stufigem Isomorphismus oder kürzer, G sei zu Γ m-stufig isomorph.

Zuerst ist es klar, dass die s' einen Theiler G' von G bilden, da jedem Producte $s_\alpha' \cdot s_\beta'$ das Product $1 \cdot 1 = 1$ entspricht. — Ferner sieht man, dass jedem $\sigma_\varkappa$ aus Γ gleichfalls m Substitutionen aus G und nur so viele entsprechen. Wenn wir nämlich mit $s_\varkappa$ eine dem $\sigma_\varkappa$ entsprechende bezeichnen, dann sind alle dem $\sigma_\varkappa$ entsprechenden durch die Producte

$$s_\varkappa s_1', \quad s_\varkappa s_2', \quad \cdots \quad s_\varkappa s_m'$$

gegeben. Dies folgt aus $\sigma_\varkappa \cdot 1 = \sigma_\varkappa$ und andrerseits aus $\sigma_\varkappa \cdot \sigma_\varkappa^{-1} = 1$. — Ebenso erkennt man, dass einem Theiler von Γ der Ordnung q ein Theiler von G der Ordnung $m \cdot q$ entspricht, und dabei einem autojugen Theiler von Γ ein autojuger Theiler von G. — Aus dieser letzten Eigenschaft ergiebt sich, dass G' ein autojuger Theiler von G ist, weil ja 1 in Γ einen autojugen Theiler bildet. — G kann nur dann in m-stufigem Isomorphismus zu Γ stehen, wenn es einen autojugen Theiler G' der Ordnung m besitzt.

Ist diese Bedingung erfüllt, dann kann eine Gruppe Γ, zu welcher G in m-stufigem Isomorphismus steht, leicht construirt werden. Es sei G' mit den Substitutionen $1, s_1', s_2', \cdots s_m'$ dieser autojuge Theiler von G, und $\varphi(z_1, \cdots z_m) = \varphi_1$ eine zu G gehörige Function. Es seien ferner

$$(12^{b}) \qquad \varphi_1, \; \varphi_2, \; \varphi_3, \; \cdots \; \varphi_t \qquad (m \cdot t = r)$$

die t Werthe, welche φ unter dem Einflusse der Substitutionen von G annimmt. Da $\varphi_\varkappa$ für $s_\varkappa^{-1} G' s_\varkappa = G'$ ungeändert bleibt, so wird die

Reihe (12^b) völlig unberührt bleiben, wenn man ein s' auf sie anwendet. Die Umwandlung von (12^b) durch ein $s_\varkappa$ wird die gleiche sein, wie durch $s_\varkappa \cdot s'$. Diese Umsetzung der $\varphi_1, \varphi_2, \cdots$ lässt sich wieder als eine Substitution $\sigma_\varkappa$ unter den Elementen φ auffassen, und so gelangt man zu der isomorphen Gruppe Γ unter den $\varphi_1, \cdots \varphi_t$, bei welcher die Einheit jeder Substitution der Gruppe G' zugeordnet ist.

Hat man eine andere Gruppe $\mathfrak{G}$, zu der G m-stufig isomorph ist, so werden natürlich $\mathfrak{G}$ und Γ einstufig-isomorph sein, falls G' in beiden Fällen der vermittelnde autojuge Theiler ist. Ist umgekehrt Γ zu $\mathfrak{G}$ einstufig-isomorph, und G zu Γ m-stufig, dann wird G zu $\mathfrak{G}$ gleichfalls m-stufig isomorph werden.

§ 559. Im § 540 haben wir gesehen, dass wenn

$$G' = [1, s_2', s_3', \cdots s_m']$$

ein Theiler der Gruppe G der Ordnung $r = mt$ ist, dann t Substitutionen $1, s_2, s_3, \cdots s_t$ bestehen, derart dass alle Substitutionen von G in die Tabelle

$$(13) \qquad \begin{array}{lllll} 1\,, & s_2'\,, & s_3'\,, & \cdots & s_m'\,; \quad G' \\ s_2\,, & s_2's_2\,, & s_3's_2\,, & \cdots & s_m's_2\,; \quad G's_2 \\ s_3\,, & s_2's_3\,, & s_3's_3\,, & \cdots & s_m's_3\,; \quad G's_3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_t\,, & s_2's_t\,, & s_3's_t\,, & \cdots & s_m's_t\,; \quad G's_t \end{array}$$

eingeordnet werden können, deren einzelne Zeilen die einzelnen conjugen Complexe $G's_\alpha$ enthalten.

Aus den Betrachtungen des vorigen Paragraphen ergiebt sich ein bedeutender Unterschied zwischen dem Falle, in welchem G' autojug in G ist, und dem, in welchem dies nicht stattfindet.

Ist G' autojug in G, dann liefert das Product einer beliebigen Substitution der $\varkappa^{\text{ten}}$ mit einer beliebigen der λ^{ten} Zeile von (13) eine Substitution einer durch $\varkappa$ und λ vermöge $s_\varkappa s_\lambda = s_\omega' s_\mu$ eindeutig bestimmten μ^{ten} Zeile. Es wird nämlich bei beliebigen α und β

$$(s_\alpha' s_\varkappa) \cdot (s_\gamma' s_\lambda) = s_\alpha' (s_\varkappa s_\beta') s_\lambda = s_\alpha' (s_\gamma' s_\varkappa) s_\lambda = s_\delta' \cdot s_\omega' s_\mu = s_\varepsilon' s_\mu .$$

Und wenn umgekehrt in (13) das Product zweier beliebiger Substitutionen der $\varkappa^{\text{ten}}$ und der λ^{ten} Zeile stets eine Substitution einer bestimmten μ^{ten} Zeile wird, dann folgt, falls man $s_\varkappa s_\lambda = s_\omega' s_\mu$ setzt, aus

$$s_\alpha' s_\varkappa \cdot s_\gamma' s_\lambda = s_\varepsilon' s_\mu ,$$

dass weiter auch

$$s'_\alpha s_\varkappa \cdot s'_\beta s_\lambda = s'_\varepsilon s'^{-1}_\omega \cdot s'_\omega s_\mu = s'_\vartheta \cdot s_\varkappa s_\lambda ,$$
$$s'_\alpha s_\varkappa s'_\beta = s'_\vartheta s_\varkappa ,$$
$$s_\varkappa s'_\beta s_\varkappa^{-1} = s'_\iota$$

wird. Lässt man nun β alle Werthe $1, 2, \cdots r$ durchlaufen, dann folgt, dass jedes $s_\varkappa$ und also auch jede Substitution von G mit G' vertauschbar und deswegen G' in G autojug ist.

Die Eigenschaft, dass die Zeilen von (13) als Elemente aufgefasst und als solche durch Vermittelung der s eindeutig componirt werden können, ist demnach charakteristisch dafür, dass G' in G autojug ist.

Nun möge dies für G und G' wirklich stattfinden. Wenden wir dann auf die Reihe der Complexe

$$G', \quad G's_2, \quad G's_3, \quad \cdots \quad G's_t$$

eine Substitution s_α an, dann geht sie in

$$G's_\alpha, \quad G's_2 s_\alpha, \quad G's_3 s_\alpha, \quad \cdots \quad G's_t s_\alpha$$

über; man erhält also eine dem s_α entsprechende Substitution

$$\sigma_\alpha = \begin{pmatrix} G's_\varkappa \\ G's_\varkappa s_\alpha \end{pmatrix} \qquad (\varkappa = 1, 2, \cdots t).$$

Bedeutet andrerseits $\varphi = \varphi_1$ eine zu G' gehörige Function, und ist

$$\varphi = \varphi_1, \quad \varphi_{s_2} = \varphi_2, \quad \varphi_{s_3} = \varphi_3, \quad \cdots \quad \varphi_{s_t} = \varphi_t,$$

dann wandelt s_α diese Folge in

$$\varphi_{s_\alpha}, \quad \varphi_{s_2 s_\alpha}, \quad \varphi_{s_3 s_\alpha}, \quad \cdots \quad \varphi_{s_t s_\alpha}$$

um; man hat also bis auf die Bezeichnung der Elemente die Substitution σ_α erhalten.

Somit erzeugt man durch die Verwendung aller s die im vorigen Paragraphen besprochene Gruppe Γ der σ, zu welcher G in m-stufigem Isomorphismus steht.

Hölder hat für diese Gruppe den Namen Factorgruppe und die Bezeichnung

$$\Gamma = G/G' \tag{14}$$

eingeführt*). Natürlich ist dabei Γ weder in der Bezeichnung noch in der Anzahl der Elemente eindeutig bestimmt; es kann, wenn ein Γ gefunden ist, jede andere dazu einstufig isomorphe Gruppe für G/G' genommen werden.

*) Math. Ann. 34 (1889), p. 26.

Jedem Theiler H von $\Gamma = G/G'$ entspricht ein Theiler H von G, dessen Ordnung m-mal so gross ist, als die von H. Aber es entspricht nicht umgekehrt jedem Theiler von G ein solcher von Γ, sondern nur denjenigen, welche G' selbst enthalten.

Wenn hierbei H autojug in Γ ist, dann wird aus

$$\Gamma^{-1}\mathsf{H}\Gamma = \mathsf{H} \quad \text{folgen} \quad G^{-1}HG = H,$$

und da H zugleich ein Multiplum von G' ist, so zeigt es sich, dass dann G' kein autojuger Maximaltheiler von G sein kann.

Umgekehrt folgt aus dem Bestehen der zweiten Gleichung die erste und damit, dass Γ nicht einfach ist. Folglich erkennt man: Die Factorgruppe $\Gamma = G/G'$ ist dann und nur dann einfach, wenn G' ein autojuger Maximaltheiler von G ist.

Siebenundfünfzigste Vorlesung.

Die Galois'sche Gruppe einer Gleichung.

§ 560. Die Kreistheilungsgleichungen und noch mehr die Abelschen Gleichungen haben uns zu der Erkenntnis geführt, dass die Aenderungen, welche gewisse Vertauschungen der Gleichungswurzeln unter einander bewirken, von Wichtigkeit für die Natur der Gleichungen selbst seien. Diese Ueberlegungen leiteten uns zunächst zur Betrachtung der cyklischen und der metacyklischen Gruppe und dann zu allgemeineren Untersuchungen über die Substitutionen selber. Wir wollen jetzt dazu übergehen, die Resultate dieser Forschungen für die Theorie beliebiger Gleichungen in voller Allgemeinheit zu verwerthen und haben dabei die aus dem Bisherigen zu schöpfenden Andeutungen zu beachten, nämlich dass die behandelten speciellen Gleichungen stets durch eine gewisse Gattung von Functionen der Wurzeln charakterisirt werden. Beispielsweise war eine cyklische Gleichung eine solche, bei welcher eine cyklische Funktion der Wurzeln zum Rationalitätsbereiche gehörte. —

Wir haben gezeigt, dass wenn $z_1, z_2, \cdots z_n$ unbestimmte Grössen sind, und wenn $\varphi(z_1, z_2, \cdots z_n)$ eine rationale Function derselben bedeutet, dann alle Substitutionen unter den z, welche φ nicht ändern, eine Gruppe bilden (§ 539). Dieser Satz lässt sich nicht auf den Fall ausdehnen, dass die $z_1, z_2, \cdots z_n$ aufhören, unbestimmte Grössen zu sein, sondern er kann versagen, sobald zwischen ihnen rationale

Beziehungen stattfinden. Hat man z. B. zwischen den drei Grössen z_1, z_2, z_3 die Relation $z_1 = z_2$, dann wird die Function

$$\varphi = z_1 + z_3,$$

welche bei unbestimmten Grössen z zu der Gruppe $[1, (z_1 z_3)]$ gehört, für die folgenden vier Substitutionen von z_1, z_2, z_3:

$$1, \ (z_1 z_2), \ (z_1 z_3), \ (z_1 z_3 z_2)$$

und nur für sie ihren Werth nicht ändern, ohne dass jedoch diese vier Substitutionen eine Gruppe bildeten. Das erklärt sich so, dass z. B. $(z_1 z_2)$ zwar nicht den Werth, wohl aber die Form von φ ändert, so dass die darauf folgende Anwendung von $(z_1 z_3)$ sich gar nicht mehr auf die vorgelegte Function φ beziehen würde.

In dem Falle also, dass die z als Wurzeln irgend einer besonderen Gleichung definirt sind

$$f(z) \equiv (z - z_1)(z - z_2) \cdots (z - z_n) = 0, \tag{1}$$

deren Coefficienten nicht mehr unabhängige Grössen sind, muss die frühere Theorie durch eine andere, allgemeinere ersetzt werden. Wir können, um dies durchzuführen, zunächst die Voraussetzung aufnehmen, dass $f = 0$ keine gleichen Wurzeln enthält. Denn sollte diese Annahme nicht erfüllt sein, dann haben wir ja Mittel an der Hand, um aus (1) eine Gleichung herzuleiten, welche jede der verschiedenen Wurzeln von (1) nur in der Multiplicität 1 enthält (§ 70; Bd. I).

Nun haben wir früher gesehen (§ 539), dass, falls nur $z_1, z_2, \cdots z_n$ unter einander verschieden sind, auch für beliebige andere Relationen zwischen ihnen bei unbestimmten $u_1, u_2, \cdots u_n$ die lineare Function

$$\varpi_1 = u_1 z_1 + u_2 z_2 + \cdots + u_n z_n \tag{2}$$

$n!$ von einander verschiedene Werthe besitzt. Diese bezeichnen wir in willkürlicher Ordnung mit

$$\varpi_1, \ \varpi_2, \ \varpi_3, \ \cdots \ \varpi_{n!}. \tag{2a}$$

Wir bilden nun, unter ϖ eine Unbestimmte verstehend, das Product

$$\gamma(\varpi) = (\varpi - \varpi_1)(\varpi - \varpi_2) \cdots (\varpi - \varpi_{n!}) \tag{3}$$

vom Grade $n!$ in ϖ. Da $\gamma(\varpi)$ in den z_λ symmetrisch ist, so gehören seine Coefficienten dem Rationalitätsbereiche an, und $\gamma(\varpi)$ ist rational darstellbar.

Hierbei ist es möglich, dass auch schon ein Factor von $\gamma(\varpi)$ rationale Coefficienten besitzt, mit anderen Worten, dass (3) reductibel ist. Dies kann infolge der besonderen Werthe der z_λ geschehen. Wir nehmen an, es sei

(4) $$g(\varpi) = (\varpi - \varpi_1)(\varpi - \varpi_2) \cdots (\varpi - \varpi_q)$$

ein solcher irreductibler Factor von (3), und zwar derjenige fest bestimmte, der den linearen Theiler $(\varpi - \varpi_1)$ enthält.

Alle Substitutionen der z_λ, welche den Werth von (4) nicht ändern, bilden eine Substitutionengruppe G. Das muss nach unseren obigen Bemerkungen über Functionen bestimmter, fester Grössen z_λ ausdrücklich bewiesen werden. Wir wollen mit g_σ das Resultat der Anwendung einer Substitution σ der z_λ auf (4) bezeichnen. Nun sei s eine Substitution, die g nicht ändert, also $g_s = g$. Weil ϖ unbestimmt ist, müssen g_s und g in allen Coefficienten und daher in allen Linearfactoren übereinstimmen; d. h. s vertauscht nur die ϖ_1, $\varpi_2, \cdots \varpi_q$ unter einander; denn die Werthe (2^a) sind ja sämmtlich unter einander verschieden.

Ist t eine andere Substitution, welche den Werth von (4) nicht ändert, so vertauscht auch t nur $\varpi_1, \varpi_2, \cdots \varpi_q$ unter einander. Daraus folgt, dass dann auch das Product st das Gleiche thut, d. h. dass $g_{st} = g_t = g$ ist. Also gehört auch st zu den Substitutionen, welche g nicht ändern; ihre Gesammtheit hat folglich, wie behauptet war, die Gruppeneigenschaft.

Daraus ergiebt sich weiter, dass die Werthe aller zu g conjugen Functionen numerisch unter sich verschieden sind. Denn hat man für irgend eine Substitution σ die numerische Beziehung $g_\sigma = g$, so blieben alle gemachten Schlüsse bestehen, und σ gehörte zu G. Wäre ferner $g_\tau = g_\sigma$, so hätte man $g_{\tau\sigma^{-1}} = g$; also gehörte $\tau\sigma^{-1}$ zu G, d. h. σ und τ wären Substitutionen eines zu G conjugen Complexes (§ 541).

Es ist demnach die Discriminante

$$\prod (g_\alpha - g_\beta) \qquad (\alpha \neq \beta)$$

von Null verschieden, und somit kann man nach § 540, (8^a) jede zur Gattung G gehörige Function rational durch g ausdrücken, d. h. eine jede solche ist gleichfalls rational bekannt.

Sind nun $s_1 = 1, s_2, \cdots s_r$ die Substitutionen der zu (4) gehörigen Substitutionengruppe G, dann gehört auch

(5) $$(\varpi - \varpi_1)(\varpi - \varpi_{s_2}) \cdots (\varpi - \varpi_{s_r})$$

zur Gattung G, weil der Complex

$$s_1 s_\alpha, \; s_2 s_\alpha, \; \cdots \; s_r s_\alpha \quad \text{mit} \quad s_1, \; s_2, \; \cdots \; s_r$$

übereinstimmt. Folglich ist (5) rational bekannt und also ein rationaler Theiler von $\gamma(\varpi)$. Gleichzeitig hat (5) mit dem irreductiblen Factor $g(\varpi)$ einen Factor $(\varpi - \varpi_1)$ gemeinsam; $g(\varpi)$ ist daher als

Factor in (5) enthalten. Andrerseits kommt jeder Factor von (5) in (4) vor, wie man sieht, wenn man auf $g(\varpi)$ alle $s_1, s_2, \cdots s_r$ anwendet und insbesondere dabei die Umwandlung von $(\varpi - \varpi_1)$ beachtet. Folglich ist (5) mit (4) identisch, und $q = r$.

Ist die Function

$$(4^a) \qquad g(\varpi) = (\varpi - \varpi_1)(\varpi - \varpi_{s_2}) \cdots (\varpi - \varpi_{s_r})$$

ein irreductibler Factor von (3), dann bilden die Substitutionen

$$s_1 = 1, \; s_2, \; \cdots \; s_r$$

eine Gruppe G, zu welcher $g(\varpi)$ gehört. Jede zur Gattung G gehörige oder unter ihr stehende Function ist rational durch $g(\varpi)$ darstellbar. —

Den letzten Satz können wir auch umkehren: Es sei $\varphi(z_1, z_2, \cdots z_n)$ eine rational bekannte Function. Da ϖ_1 zur Galois'schen Gattung gehört und deswegen auch eine von Null verschiedene Discriminante besitzt, so kann jede Function der z_λ durch ϖ_1 rational ausgedrückt werden. Insbesondere gelte für unsere Function

$$\varphi(z_1, z_2, \cdots z_n) = P(\varpi_1).$$

Dann hat die Gleichung in ϖ, deren Coefficienten rational bekannt sind,

$$P(\varpi) - \varphi = 0 \quad \text{mit} \quad g(\varpi) = 0$$

die Wurzel ϖ_1 gemeinsam und, da g irreductibel ist, alle Wurzeln. Demgemäss gilt auch

$$\varphi = P(\varpi_1) = P(\varpi_{s_2}) = \cdots = P(\varpi_{s_r}),$$

oder mit anderen Worten: $\varphi(z_1, \cdots z_n)$ bleibt für alle Substitutionen von G ungeändert, d. h.: Jede rational bekannte Function $\varphi(z_1, z_2, \cdots z_n)$ gehört zur Gruppe G oder steht unter ihr.

Dieses letzte Theorem lässt auch noch eine andere, häufig nützliche Fassung zu: Jede rationale Relation, die zwischen den Wurzeln $z_1, z_2, \cdots z_n$ besteht, bleibt richtig, wenn in ihr auf die z die Substitutionen von G angewendet werden. Denn eine jede solche Relation lässt sich in die Form $\varphi = 0$ bringen.

So zeigt sich die grosse Bedeutung dieser Gruppe G oder ihrer Gattung für (1). Wir nennen G die Galois'sche Gruppe*) oder kürzer die Gruppe der Gleichung (1).

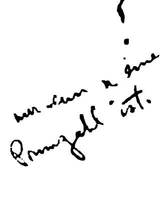
*) Oeuvres d'Évariste Galois, édit. p. Picard, p. 33. Die Abhandlung stammt aus dem Jahre 1831.

Da $g(\varpi)$ nur für G ungeändert bleibt, so ist es charakteristisch für jede Substitution der Gruppe, dass ihre Anwendung jede Function numerisch ungeändert lässt, welche sich rational darstellen lässt.

Hat also die irreductible Gleichung $f(z)=0$ reelle Coefficienten, und besteht auch der Rationalitätsbereich aus reellen Grössen, sind ferner $z_1, z_2; z_3, z_4; \cdots; z_{2\varkappa-1}, z_{2\varkappa}$ die $\varkappa$ Paare conjugirt complexer Wurzeln, welche $f(z)=0$ besitzt; und bedeutet endlich $\varphi(z_1, z_2, \cdots z_n)$ eine jede rational bekannte Function, so wird φ seinen Werth nicht ändern, wenn das in $z_1, z_2, \cdots z_{2\varkappa}$ auftretende Symbol $\sqrt{-1}$ in $-\sqrt{-1}$ verwandelt, d. h. wenn jede der complexen Wurzeln durch ihre conjugirt complexe ersetzt wird. Diese Umänderung ist einer Substitution

$$s = (z_1 z_2)(z_3 z_4)\cdots(z_{2\varkappa-1} z_{2\varkappa})$$

äquivalent; folglich gehört diese zur Gruppe der Gleichung*). Wenn also insbesondere $f(z)=0$ nur die beiden complexen Wurzeln z_1 und z_2 enthält, dann gehört $s=(z_1 z_2)$ zu der Gruppe. Daraus kann man (§ 519 und § 567) schliessen, dass die Gruppe einer irreductiblen numerischen Gleichung, welche nur zwei complexe Wurzeln besitzt, mit der symmetrischen Gruppe der Wurzeln zusammenfällt; d. h. die Gleichung ist so beschaffen, dass nur die symmetrischen Functionen ihrer Wurzeln rational bekannt sind. Könnte man also zeigen, dass es in einem gegebenen reellen Rationalitätsbereiche irreductible Gleichungen n^{ten} Grades mit nur zwei complexen Wurzeln giebt, so wäre bewiesen, dass diese als Gruppe die symmetrische Gruppe besitzen. (Vgl. hierüber weiter § 566.)



§ 561. Es sei nun σ eine Substitution der z, welche nicht in G enthalten ist; sie möge ϖ_1 in ϖ_σ umwandeln. Wir bilden

$$(6) \qquad (\varpi-\varpi_\sigma)(\varpi-\varpi_{\sigma s_2})\cdots(\varpi-\varpi_{\sigma s_r}).$$

Dieses Product gehört zur Gattung G und ist also rational darstellbar. Ferner hat es mit (5) keinen linearen Factor gemeinsam, weil alle σs_α von den s_α verschieden sind. Endlich kommt jeder seiner Factoren in (3) vor. Folglich ist (6), genau wie $g(\varpi)$, ein rationaler Theiler von $\gamma(\varpi)$. (6) ist auch irreductibel. Denn könnte man es in rationale Factoren niederen Grades zerspalten, so wäre es möglich, einen derselben zum Ausgangspunkte der Untersuchung des vorigen Paragraphen zu wählen, und man käme statt auf die Gattung G auf eine andere

*) E. Maillet, Mém. de l'Assoc. franç. pour l'Avancem. des Sciences (1897). — C. R. 127 (1898), p. 1004.

mit geringerer Gruppe, was nicht möglich ist, weil sonst $g(\varpi)$ zerlegbar würde.

Die Bildung von (6) zeigt, dass die Gattung, zu der man von dieser Function aus gelangt, die gleiche ist, wie diejenige, welche (4) liefert. Es ist demnach gleichgültig, von welchem der irreductiblen Factoren von $\gamma(\varpi)$ man ausgeht.

Ist $n! > 2r$, dann kann man in derselben Weise das Verfahren fortsetzen. Zerfällt (3), dann sind alle seine Factoren von demselben Grade r, und sie gehören sämmtlich derselben Gruppe G an.

Es mag noch darauf aufmerksam gemacht werden, dass (6) nicht etwa ein zu (4) conjuger Werth ist. Ein solcher würde, wenn er $(\omega - \omega_\sigma)$ enthalten sollte, gleich

$$(\varpi - \varpi_\sigma)(\varpi - \varpi_{s_2\sigma}) \cdots (\varpi - \varpi_{s_r\sigma})$$

sein, und die zugehörige Gruppe wäre i. A. von G verschieden.

§ 562. Wenn durch (1) die Gleichung

$$f(z) \equiv z^n - c_1 z^{n-1} + c_2 z^{n-2} - \cdots \pm c_n = 0 \tag{1^a}$$

gegeben ist, dann wird natürlich dadurch zugleich G bestimmt, ebenso wie der Complex der Wurzeln $z_1, \cdots z_n$. Aber man kann die Natur der Gleichung (1ª) immer noch dadurch ändern, dass man gewisse Beziehungen zwischen den Wurzeln festsetzt. Dies ist natürlich nur so möglich, dass diese Beziehungen in Uebereinstimmung mit den Wurzelwerthen stehen, und daher können sich solche Beziehungen auch nur auf den Rationalitätsbereich beziehen. Ihr Wesen kann somit nur darin bestehen, dass der Rationalitätsbereich durch sie über die symmetrischen Functionen hinaus erweitert wird. Jede Function der Wurzeln ist ja numerisch bestimmt, sobald (1ª) gegeben ist. Aber man kann sie zum Rationalitätsgebiete hinzunehmen, sie diesem, wie man sagt, adjungiren und dadurch die Natur der Gleichung ändern. Das wird folglich dadurch und nur dadurch geschehen können, dass eine vorher nicht rational bekannte Function $h(z_1, \cdots z_n)$ als rational angesehen und dem bisherigen Rationalitätsbereiche $(\mathfrak{R}', \mathfrak{R}'', \cdots)$ hinzugefügt, ihm adjungirt wird.

Schon an den Gleichungen zweiten Grades lässt sich dies exemplificiren.

Es sei die irreductible Gleichung zweiten Grades

$$z^2 - 2az + b = 0$$

gegeben; wir setzen

$$\varpi_1 = u_1 z_1 + u_2 z_2, \quad \varpi_2 = u_1 z_2 + u_2 z_1,$$

$$\gamma(\varpi) = \varpi^2 - 2a(u_1 + u_2)\varpi + (u_1 - u_2)^2 b + 4a^2 u_1 u_2 = 0.$$

Im Allgemeinen ist $\gamma(\varpi)$ unzerlegbar. Wir haben nun als rational bekannt die symmetrische Function

$$(z_1 - z_2)^2 = 4(a^2 - b);$$

setzen wir $a^2 - b = c_0^2$ und nehmen c_0 in den Rationalitätsbereich auf, dann entsteht

$$z_1 - z_2 = 2c_0,$$

und jetzt zerfällt, wie man leicht sieht, $\gamma(\varpi)$ in zwei lineare Factoren. Hier wäre es noch möglich gewesen, die Bestimmung $a^2 - b = c_0^2$ in die quadratische Gleichung selbst aufzunehmen, indem man sie unter Einführung von c_0 an Stelle von b

$$z^2 - 2az + b = z^2 - 2az + a^2 - c_0^2 = 0$$

schreibt. Aber es ist nicht unwahrscheinlich, dass unter etwas complicirteren Annahmen eine solche Uebertragung der Thatsache, dass eine Function $h(z_1, \cdots z_n)$ als bekannt angesehen werden soll, in die Gleichung selbst auf rationalem Wege nicht mehr durchführbar ist.

§ 563. In besonders einfachen Fällen kann man durch Vermittelung der Wurzeln selbst die Gleichungsform, welche zu einer gegebenen Gruppe gehört, berechnen. Wir wollen dies an den Gleichungen vierten Grades für einige Gruppen zeigen.

Zunächst sei die cyklische Gruppe

$$G = [1, (z_1 z_2 z_3 z_4), (z_1 z_3)(z_2 z_4), (z_1 z_4 z_3 z_2)]$$

die Gruppe einer Gleichung $f(z) = 0$ des vierten Grades. Dann wissen wir aus früheren Untersuchungen, dass diese Gleichung cyklisch und dass die Functionen

$$(z_1 - iz_2 - z_3 + iz_4)^4, \quad (z_1 + iz_2 - z_3 - iz_4)^4$$

als Lagrange'sche Resolventen rational bekannt sind. Zugleich erkennt man, dass jede dieser Functionen zu G gehört und nicht zugleich unter G steht. Ferner sieht man, dass auch

$$(z_1 - iz_2 - z_3 + iz_4)(z_1 + iz_2 - z_3 - iz_4)$$

zu G gehört. Man kann also mit rationalem b und s

$$z_1 - iz_2 - z_3 + iz_4 = 4\sqrt[4]{b}, \quad z_1 + iz_2 - z_3 - iz_4 = 4s\sqrt[4]{b^3}$$

setzen; nur darf b keine vierte Potenz im Rationalitätsbereiche sein.

Ferner gehört $(z_1 - z_2 + z_3 - z_4)^2$ zu G und ist also im Rationalitätsbereiche enthalten. Ebenso ist aber auch

$$(z_1 - z_2 + z_3 - z_4)(z_1 - iz_2 - z_3 + iz_4)^2$$

zu G gehörig; deshalb können wir mit rationalem r

$$z_1 - z_2 + z_3 - z_4 = 4r\sqrt[4]{b^2}$$

setzen. Wenn wir dann endlich die symmetrische Function

$$z_1 + z_2 + z_3 + z_4 = 4a$$

zu Hülfe nehmen, dann ergiebt sich durch Combination der vier in den z linearen Gleichungen als Resultat

$$(7)\qquad \begin{aligned} z_1 &= a + \sqrt[4]{b} + r\sqrt[4]{b^2} + s\sqrt[4]{b^3}, \\ z_2 &= a + i\sqrt[4]{b} - r\sqrt[4]{b^2} - is\sqrt[4]{b^3}, \\ z_3 &= a - \sqrt[4]{b} + r\sqrt[4]{b^2} - s\sqrt[4]{b^3}, \\ z_4 &= a - i\sqrt[4]{b} - r\sqrt[4]{b^2} + is\sqrt[4]{b^3}; \end{aligned}$$

und daraus findet man für $y_x = z_x - a$ die Gleichung mit den Wurzeln y_1, y_2, y_3, y_4

$$y^4 - 2b(2s + r^2)y^2 - 4br(1 + bs^2)y + b^2(r^2 - 2s)^2 - b(1 + bs^2)^2 = 0$$

als allgemeine cyklische Gleichung vierten Grades mit verschwindendem zweiten Gliede.

Abel hat in einem Briefe an Crelle vom 14. März 1826

$$m + n\sqrt{1 + e^2} + \sqrt{h(1 + e^2 + \sqrt{1 + e^2})}$$

als Wurzelform angegeben. Wir gelangen von (7) zu ihr, wenn wir

$$i\sqrt[4]{b} - is\sqrt[4]{b^3} = \left[\frac{(1 + bs^2)^2}{2s}\left(\frac{4bs^2}{(1 + bs^2)^2} - \sqrt{\frac{4bs^2}{(1 + bs^2)^2}}\right)\right]^{\frac{1}{2}},$$

$$h = \frac{(1 + bs^2)^2}{2s}, \quad e = i\,\frac{1 - bs^2}{1 + bs^2}$$

setzen. —

Wir stellen uns zweitens das Problem, die Gleichungen vierten Grades mit der Gruppe

$$H = [1, (z_1z_2)(z_3z_4), (z_1z_3)(z_2z_4), (z_1z_4)(z_2z_3)]$$

zu finden. Hier ist das Product

$$(z_1 + z_2 - z_3 - z_4)(z_1 - z_2 + z_3 - z_4)(z_1 - z_2 - z_3 + z_4)$$

und ebenso das Quadrat jedes einzelnen Factors in diesem Product zu H gehörig. Wir können deshalb die Werthe der Factoren gleich

$\sqrt{b}$, $\sqrt{c}$, $d\sqrt{bc}$ setzen, wobei b, c keine Quadrate im Rationalitätsbereiche sein dürfen und b, c, d rational sind. Wir finden wie oben, falls $z_1 + z_2 + z_3 + z_4 = 4a$ gesetzt wird,

$$\begin{aligned} z_1 &= a + \sqrt{b} + \sqrt{c} + d\sqrt{bc}, \\ z_2 &= a + \sqrt{b} - \sqrt{c} - d\sqrt{bc}, \\ z_3 &= a - \sqrt{b} + \sqrt{c} - d\sqrt{bc}, \\ z_4 &= a - \sqrt{b} - \sqrt{c} + d\sqrt{bc}. \end{aligned} \tag{8}$$

Setzt man auch hier wieder $y_\varkappa = z_\varkappa - a$, so entsteht

$$y^4 - 2(b + c + bcd^2)y^2 - 8bcdy + (b - c - bcd^2)^2 - 4bc^2d^2 = 0.$$

Diese Gleichung löst die gestellte Aufgabe. —

Wir untersuchen endlich drittens die Gleichungen vierten Grades mit der Gruppe

$$K = [1,\ (z_1z_2z_3z_4),\ (z_1z_3)(z_2z_4),\ (z_1z_4z_3z_2),$$
$$(z_1z_3),\ (z_1z_2)(z_3z_4),\ (z_2z_4),\ (z_1z_4)(z_2z_3)].$$

Hier ist $(z_1 - z_3)^2 + (z_2 - z_4)^2$ rational bekannt; wir setzen es $= 8c$; ebenso ist

$$[(z_1 - z_3)^2 - (z_2 - z_4)^2]^2$$

für die Gruppe K unveränderlich und kann daher $= 4^3 b$, d. h.

$$(z_1 - z_3)^2 - (z_2 - z_4)^2 = 8\sqrt{b}$$

genommen werden; b darf kein Quadrat sein. Es folgt

$$(z_1 - z_3)^2 = 4(c + \sqrt{b}), \quad (z_2 - z_4)^2 = 4(c - \sqrt{b}).$$

Weiter ist $(z_1 - z_2 + z_3 - z_4)^2$ zu K gehörig und ebenso ist es $[(z_1 - z_3)^2 - (z_2 - z_4)^2](z_1 - z_2 + z_3 - z_4)$; demnach wird

$$z_1 - z_2 + z_3 - z_4 = 4d\sqrt{b},$$

und setzen wir endlich

$$z_1 + z_2 + z_3 + z_4 = 4a,$$

so folgt, wenn man wieder $y_\varkappa = z_\varkappa - a$ schreibt,

$$\begin{aligned} z_1 &= a + d\sqrt{b} + \sqrt{c + \sqrt{b}}, \quad & z_3 &= a + d\sqrt{b} - \sqrt{c + \sqrt{b}}; \\ z_2 &= a - d\sqrt{b} + \sqrt{c - \sqrt{b}}, \quad & z_4 &= a - d\sqrt{b} - \sqrt{c - \sqrt{b}}; \end{aligned} \tag{9}$$

$$y^4 - 2(bd^2 + c)y^2 - 4bdy + (bd^2 - c)^2 - b = 0.$$

Hierbei müssen a, b, c, d rational sein, und b darf kein Quadrat werden.

Ueber die Aufgaben dieses Paragraphen vgl. H. Weber, Marburg. Ber. 1892 und Fr. Hack, Dissertation, Tübingen 1895.

Wir kehren nunmehr zu allgemeineren Betrachtungen zurück.

§ 564. Unsere Ueberlegungen haben uns gezeigt, dass der Gleichung (1) durch Hinzufügung, Adjunction, einer als rational anzusehenden Function

$$(10) \qquad h(z_1, z_2, \cdots z_n)$$

eine neue besondere Eigenschaft verliehen werden kann, dass sie dadurch nach der Kronecker'schen Ausdrucksweise einen Affect erhält. Eine solche Hinzufügung hat natürlich nur dann einen Nutzen, wenn die Gattung von h nicht schon mit der Gattung G zusammenfällt oder unter ihr steht. Denn in diesem Falle würde ja (10) bereits vor der Adjunction bekannt sein. Ist aber eine solche Function (10) dem Rationalitätsbereiche adjungirt worden, dass dieser dadurch eine Erweiterung erfahren hat, dann geht die Zerfällung von $\gamma(\varpi)$ noch über $g(\varpi)$ hinaus vor sich. Es wird $g(\varpi)$ nämlich durch die Adjunction von (10) reductibel.

Um dies zu zeigen, wollen wir unter $q(z_1, z_2, \cdots z_n)$ eine zu G gehörige Function und ferner unter H die zu $h(z_1, z_2, \cdots z_n)$ gehörige Gruppe verstehen. Dann ist die Function

$$k(z_1, \cdots z_n) = q(z_1, z_2, \cdots z_n) + v \cdot h(z_1, z_2, \cdots z_n)$$

bei unbestimmten v rational bekannt. Diese Function gehört zu der aus den gemeinsamen Substitutionen von G und H bestehenden Gruppe K. Man sieht sofort, dass diese Substitutionen eine Gruppe bilden (§ 539, Schluss); und ferner ist es klar, dass k nur dann ungeändert bleibt, wenn g und h es bleiben. Es ist sonach jede zu K gehörige Function rational darstellbar.

Wenn man nun auf den Factor $(\varpi - \varpi_1)$ alle Substitutionen von K anwendet und das Product der entstehenden Factoren bildet, so erhält man folglich einen rational bekannten Factor von $g(\varpi)$. Dabei zerfällt $g(\varpi)$ wieder in Factoren gleicher Grade, von denen jeder einzelne zu der Gruppe K gehört.

Hierdurch ist zugleich gezeigt worden, dass es bei jeder Adjunction ausreicht, für h eine Function zu wählen, deren Gruppe H ein Theiler von G wird, so dass $g(\varpi)$ unter $h(z_1, z_2, \cdots z_n)$ steht.

Weiter ist es ersichtlich, dass nur dann eine Adjunction den Affect der Gleichung ändert, wenn durch sie $g(\varpi)$ reductibel wird.

Endlich erkennt man, dass der scheinbar allgemeinere Fall der Adjunction zweier oder mehrerer Functionen $h(z_1, \cdots z_n)$, $\eta(z_1, \cdots z_n), \cdots$ mit dem eben besprochenen identisch wird, sobald man die eine Function

$$(11) \qquad h(z_1, z_2, \cdots z_n) + v \cdot \eta(z_1, z_2, \cdots z_n)$$

adjungirt.

In (10) und in (11) haben wir der Einfachheit des Beweises halber eine Unbestimmte v eingeführt. Man kann diese aber auch durch eine passend gewählte Constante ersetzen. Es kommt nämlich bei dem Beweise nur darauf an, wenn h_α, h_β und η_α, η_β conjuge Functionen sind, die Wahl so zu treffen, dass aus dem Bestehen der Gleichung

$$h_\alpha(z_1, \cdots z_n) + v\eta_\alpha(z_1, \cdots z_n) = h_\beta(z_1, \cdots z_n) + v\eta_\beta(z_1, \cdots z_n)$$

der Schluss $\alpha = \beta$ gezogen werden darf. Ist nun M das Maximum, welches der absolute Betrag $|h_\alpha - h_\beta|$, und m das Minimum, welches $|\eta_\alpha - \eta_\beta|$ für alle möglichen α und β annehmen kann, und wählt man die Constante

$$v > \frac{M}{m},$$

dann ist offenbar die gestellte Bedingung erfüllt.

§ 565. Wir wollen jetzt den Hilbert'schen Irreductibilitätssatz benutzen, um ein wichtiges Theorem über die Galois'sche Gruppe einer Gleichung herzuleiten (vgl. Hilbert, Journ. f. Math. 110 [1892] p. 123).

Es sei eine Gleichung n^{ten} Grades in z vorgelegt von der Gestalt

$$F_0 z^n + F_1 z^{n-1} + \cdots + F_n = 0,$$

deren Coefficienten $F_0, F_1, \cdots F_n$ ganze rationale Functionen der Parameter $t, r, \cdots q$ mit ganzen rationalen Zahlencoefficienten sind. Um die Gruppe G der Gleichung in dem durch die rationalen Zahlen und die Parameter $t, r, \cdots q$ bestimmten Rationalitätsbereiche zu finden, bilden wir, wenn $z_1, z_2, \cdots z_n$ die Wurzeln der vorgelegten Gleichung sind, $\gamma(\varpi)$. Dieser Ausdruck wird nach der Multiplication mit der $(n!)^{\text{ten}}$ Potenz von F_0 eine ganze, ganzzahlige Function der Unbestimmten $\varpi, u_1, u_2, \cdots u_n, t, q, \cdots r$. Ist nun $g(\varpi)$ ein ganzer, ganzzahliger, im Bereiche der rationalen Zahlen irreductibler Factor von $\gamma(\varpi)$, so wird die gesuchte Gruppe G durch diejenigen Substitutionen gebildet, welche $g(\varpi)$ ungeändert lassen. Wir wollen jetzt zeigen: Man kann in die vorgelegte Gleichung auf unendlich viele Arten für die Parameter $t, r, \cdots q$ ganze rationale Zahlen derart einsetzen, dass die so entstehende ganzzahlige Gleichung im Bereiche der rationalen Zahlen die nämliche Gruppe G besitzt wie bei unbestimmten Parametern.

Nach dem Hilbert'schen Theorem (§ 487) können wir zunächst für t unbegrenzt viele ganze rationale Zahlen bestimmen, nach deren Einsetzung $g(\varpi)$ eine im Bereiche der rationalen Zahlen irreductible Function der Veränderlichen $\varpi, u_1, \cdots u_n, r, \cdots q$ wird. Dies allein

reicht aber für unsere Zwecke noch nicht aus, denn es könnte dabei die vorgelegte Gleichung gleiche Wurzeln erhalten. Um dies zu vermeiden, berechnen wir die Discriminante D der vorgelegten Gleichung; dieselbe wird nach Multiplication mit einer Potenz von F_0 eine ganze, ganzzahlige, nicht identisch verschwindende Function der Parameter $t, r, \cdots q$. Es giebt bei unbestimmten $r, \cdots q$ nur eine endliche Werthezahl von t, für welche die Discriminante verschwindet; diese erhält man, wenn man die Discriminante nach Potenzproducten der $r, \cdots q$ entwickelt und die einzelnen Coefficienten, welche Functionen von t werden, gleich Null setzt. Wir verfügen nun über unbegrenzt viele Zahlen t, welche $g(\varpi)$ irreductibel lassen; folglich existiren auch unbegrenzt viele, die zugleich $D \neq 0$ lassen. Eine von diesen t_0 wählen wir aus.

Hierauf bestimmen wir eine ganze rationale Zahl r_0, bei deren Einsetzung für r die Function $g(\varpi)$ eine im Bereiche der rationalen Zahlen irreductible Function der übrig bleibenden Veränderlichen wird, und für welche überdies die Discriminante D von Null verschieden bleibt.

So fortfahrend erhalten wir für $t, r, \cdots q$ ganze rationale Zahlen $t_0, r_0, \cdots q_0$, nach deren Einsetzung eine ganzzahlige irreductible Function $g_0(\varpi)$ der Unbestimmten $\varpi, u_1, u_2, \cdots u_n$ herauskommt, und für welche die Discriminante D der Gleichung eine von Null verschiedene rationale Zahl wird.

Es ist nun einerseits offenbar, dass alle Substitutionen, welche $g(\varpi)$ ungeändert lassen, auch $g_0(\varpi)$ nicht ändern werden; andrerseits kann $g_0(\varpi)$ bei keinen anderen Substitutionen ungeändert bleiben, da die Ordnung der Gruppe mit dem Grade von g oder g_0 in ϖ übereinstimmt. G ist mithin zugleich die Gruppe der durch Einsetzung jener ganzen Zahlen entstehenden ganzzahligen Gleichung.

§ 566. Von dem allgemeinen Satze des vorigen Paragraphen wollen wir eine Anwendung machen, indem wir für $F_0, F_1, \cdots F_n$ selbst die Parameter $t, r, \cdots q$, d. h. also unbestimmte Grössen eintragen. In diesem Falle ist $\gamma(\varpi)$ irreductibel, und G wird zur symmetrischen Gruppe. Denn gesetzt, $\gamma(\varpi)$ zerfiele, so wäre, wie in dieser Vorlesung gezeigt wurde, eine rationale, nicht symmetrische Function der Wurzeln bekannt. Dies können wir durch

$$h(z_1, z_2, \cdots z_n) = 0$$

ausdrücken. Daraus würde folgen, dass das auf alle conjugen Werthe erstreckte symmetrische Product

$$F_0^{\varrho} \prod h(z_{i_1}, z_{i_2}, \cdots z_{i_n}) = H(F_0, F_1, \cdots F_n) = 0$$

wäre. Da $H = 0$ für unbestimmte Parameter gilt, so muss H identisch gleich Null sein; also auch Πh; folglich auch einer der Factoren, für den wir, da es sich nur um Aenderung der Bezeichnung handelt, $h(z_1, z_2, \cdots z_n)$ nehmen können. Gegen die Annahme wäre also h identisch Null und stellte also keine Function dar, die zu einer unter der symmetrischen enthaltenen Gattung gehörte.

Daraus folgt, dass es unbegrenzt viele Gleichungen n^{ten} Grades mit ganzzahligen Coefficienten giebt, deren Gruppe im Bereiche der rationalen Zahlen die symmetrische Gruppe ist; diese haben demnach keinen Affect.

Achtundfünfzigste Vorlesung.

Transitivität und Primitivität.

§ 567. Um die Wichtigkeit der Gruppe einer Gleichung für die Erkenntniss der Natur dieser Gleichung noch von einer anderen Seite her ersichtlich zu machen, wollen wir den Einfluss von Reductibilität und Irreductibilität auf die Constitution der Gruppe betrachten.

Es sei $f(z) = 0$ gegeben, und der Rationalitätsbereich möge durch

$$(h(z_1, \cdots z_n), \mathfrak{R}_1, \mathfrak{R}_2, \cdots) \tag{1}$$

bestimmt sein. In ihm möge $f(z)$ reductibel werden, und zwar sei

$$\begin{aligned} f(z) &= p(z) \cdot q(z); \\ p(z) &= (z - z_1)(z - z_2) \cdots (z - z_a); \\ q(z) &= (z - z_{a+1})(z - z_{a+2}) \cdots (z - z_n). \end{aligned} \tag{2}$$

Ferner bezeichnen wir die Gruppe von f in (1) mit G.

Da $p(z)$ rational bekannt ist, so bleibt es unter der Einwirkung von G ungeändert, d. h. keine der Substitutionen von G ist im Stande, ein $z_1, z_2, \cdots z_a$ in ein $z_{a+1}, z_{a+2}, \cdots z_n$ umzuwandeln. Die Substitutionen von G sind also so beschaffen, dass sie nur $z_1, z_2, \cdots z_a$ unter sich und ebenso nur $z_{a+1}, z_{a+2}, \cdots z_n$ unter sich vertauschen.

Umgekehrt möge G die Eigenschaft haben, dass seine Substitutionen $s_1 = 1, s_2, \cdots s_r$ auf z_1 nur einen der Werthe $z_1, z_2, \cdots z_a$ folgen lassen; dann vertauschen sie die $z_1, z_2, \cdots z_a$ überhaupt nur unter sich. Wendet man alle auf das Product

$$(z - z_1)(z - z_2) \cdots (z - z_a)$$

an, dann bleibt dies hierfür ungeändert und ist folglich rational darstellbar. Es ist demnach $p(z)$ rational bekannt, und $f(z)$ reductibel.

Kennt man mithin die Galois'sche Gruppe einer Gleichung, so weiss man sofort, ob die Gleichung reductibel oder irreductibel ist. Die Gruppe einer Zahlengleichung ist im Gebiete sämmtlicher complexer Zahlen gleich 1.

Wir nennen eine Gruppe transitiv, wenn es durch ihre Substitutionen möglich ist, auf z_1 jedes andere Element $z_1, z_2, \cdots z_n$ folgen zu lassen, und intransitiv, wenn die Gruppe diese Eigenschaft nicht besitzt*). Mit Hülfe dieser Einführung können wir sagen: Für die Irreductibilität einer Gleichung in irgend einem Rationalitätsbereiche ist die Transitivität ihrer für diesen Bereich bestehenden Gruppe charakteristisch.

In § 68, Bd. I sahen wir, dass wenn eine Function $g(z)$ für die Wurzel z_1 einer irreductiblen Gleichung $f(z)=0$ verschwindet, Gleiches für alle Wurzeln von $f=0$ eintritt. Dieser Satz zeigt sich jetzt als besonderer Fall des Theorems von § 560, S. 347; denn ist $g(z_1)\equiv 0$, so erlauben es die Substitutionen der Gruppe G von f, die Wurzel z_1 der Reihe nach durch alle anderen Wurzeln zu ersetzen.

§ 568. Als Beispiele für die Bildung der Gruppe einer Gleichung und ihren Charakter für die Transitivität oder Intransitivität wollen wir zwei besonders wichtige Fälle besprechen. Wir suchen zunächst die Gruppe einer Gleichung auf, welche irreductibel und so beschaffen ist, dass alle ihre Wurzeln rational durch eine unter ihnen darstellbar sind; wir können hier also setzen

$$z_1,\quad z_2=\varphi_2(z_1),\quad z_3=\varphi_3(z_1),\quad \cdots\quad z_n=\varphi_n(z_1). \tag{3}$$

Da die Werthe der einzelnen Differenzen

$$z_2-\varphi_2(z_1),\quad z_3-\varphi_3(z_1),\quad \cdots$$

gleich Null und mithin bekannt sind, so müssen sie ungeändert bleiben, falls man eine Substitution s der Gleichungsgruppe auf sie anwendet. Führt diese Substitution s_i die Wurzel z_1 in z_i über, so sind demnach auch

$$z_i,\quad \varphi_2(z_i),\quad \varphi_3(z_i),\quad \cdots\quad \varphi_n(z_i) \tag{4}$$

Wurzeln von $f(z)=0$. Diese Grössen sind nun sämmtlich unter einander verschieden; denn aus einer Relation

$$\varphi_\alpha(z_i)=\varphi_\beta(z_i)\quad \text{würde folgen}\quad \varphi_\alpha(z_1)=\varphi_\beta(z_1),$$

falls man die inverse Substitution verwendet oder falls man die Irreductibilität von f berücksichtigt; $\varphi_\alpha(z_1)=\varphi_\beta(z_1)$ ist aber wegen

*) Kronecker (Grundzüge § 12) nennt Gattungen mit transitiver Gruppe „eigentliche", diejenigen mit intransitiver Gruppe „uneigentliche Gattungen".

(3) und der Irreductibilität von f ausgeschlossen. Folglich sind die obigen Grössen alle von einander verschieden; d. h. die Reihe (4) liefert alle Wurzeln, genau wie (3). Daraus folgt mithin, dass alle Wurzeln durch eine jede beliebige rational ausgedrückt werden können.

Keine Substitution, welche z_1 etwa in z_i umwandelt, lässt ein $z_x = \varphi_x(z_1)$ ungeändert, denn sonst wäre auch

$$\varphi_x(z_1) = \varphi_x(z_i).$$

Infolge dessen würden die Schlüsse von § 489 zeigen, dass die niedrigste Iteration der Reihe

$$\varphi_x(z_1) = \varphi_x(z_i), \quad \varphi_x[\varphi_x(z_1)] = \varphi_x[\varphi_x(z_i)], \ \cdots,$$

welche den Werth z_1 hervorruft, auch z_i wieder liefert und umgekehrt, so dass $z_1 = z_i$ wird.

Daraus ergiebt sich, dass jede Substitution s aus G, welche z_1 umsetzt, alle Elemente $z_1, z_2, \cdots z_n$ an neue Stellen setzt.

Wäre nun $t = (z_a)(z_b z_c \cdots) \cdots$ eine Substitution von G, die ein beliebiges Element z_a nicht umsetzt, ohne dass doch $t = 1$ wäre, so nehmen wir eine Substitution s aus G, die auf z_a folgen lässt z_1. Eine solche ist wegen der Transitivität von G sicher vorhanden. Wir bilden $s^{-1}ts$ und beachten, dass diese Transformirte nun z_1 nicht ändert. Da dies Resultat unseren letzten Ergebnissen entgegen ist, so kann kein solches t bestehen. Folglich setzt jede Substitution von G ausser der Einheit alle Wurzeln um.

Wenn umgekehrt für eine transitive Gleichungsgruppe G diese Eigenschaft gilt, dann kann man jede ihrer Wurzeln durch jede andere z_a rational darstellen. Adjungiren wir nämlich z_a dem Rationalitätsgebiete, dann geht die Gleichungsgruppe in denjenigen ihrer Theiler über, welcher z_a ungeändert lässt (§ 564). Dieser Theiler wird nach den jetzigen Darlegungen nur aus der identischen Substitution 1 bestehen. Folglich ist im neuen Rationalitätsbereiche jede rationale Function der Wurzeln enthalten, und im Besonderen sind $z_1, z_2, \cdots z_n$ rationale Functionen von z_a.

Weiter erkennt man, dass G nur n Substitutionen hat, je eine nämlich, die z_1 in $z_1, z_2, \cdots z_n$ überführt. Denn liefern s und s' dieselbe Umsetzung von z_1, dann lässt $s^{-1}s'$ das z_1 ungeändert.

Endlich ist es klar, dass jede Substitution von G regelmässig sein wird, d. h. dass jeder ihrer Cyklen von gleicher Ordnung ist. Denn im entgegengesetzten Falle würden geeignete Potenzen, ohne $= 1$ zu werden, gewisse Wurzeln nicht umstellen.

So sehen wir: Für eine irreductible Gleichung n^{ten} Grades, deren Wurzeln sämmtlich rational durch eine bestimmte unter ihnen darstellbar sind, ist es charakteristisch, dass ihre Galois'sche Gruppe G transitiv, von der Ordnung n und so beschaffen ist, dass jede Substitution mit Ausnahme der identischen alle Wurzeln umstellt; es sind alle Substitutionen der Gruppe G regulär.

Daraus folgt insbesondere noch, dass wenn n eine Primzahl p wird, dann die Gruppe aus den Potenzen einer cyklischen Substitution besteht. —

Für $n = 4$ giebt es zwei Typen derartiger Gruppen. Es sind dies die in § 563 behandelten

$$G = [1,\ (z_1 z_2 z_3 z_4),\ (z_1 z_3)(z_2 z_4),\ (z_1 z_4 z_3 z_2)];$$
$$H = [1,\ (z_1 z_2)(z_3 z_4),\ (z_1 z_3)(z_2 z_4),\ (z_1 z_4)(z_2 z_3)].$$

Ebenso hat man für $n = 6$ zwei Typen, von denen der eine die Potenzen einer cyklischen Substitution umfasst, während der zweite aus den sechs Substitutionen besteht

$$1,\ (z_1 z_2 z_3)(z_4 z_5 z_6),\ (z_1 z_3 z_2)(z_4 z_6 z_5),$$
$$(z_1 z_4)(z_2 z_6)(z_3 z_5),\ (z_1 z_5)(z_2 z_4)(z_3 z_6),\ (z_1 z_6)(z_2 z_5)(z_3 z_4).$$

Zu den behandelten Gleichungen gehören die in § 560 besprochenen $\gamma(\varpi) = 0$ mit den Wurzeln

$$\varpi_i = u_1 z_{i_1} + u_2 z_{i_2} + \cdots + u_n z_{i_n},$$

falls sie irreductibel sind; sonst ihre irreductiblen Theiler $g(\varpi) = 0$, die uns gerade auf die Gruppe G der Gleichung geführt haben. Wir können also jeder Gleichung $f(z) = 0$ eine solche Galois'sche Gleichung $g(\varpi) = 0$ zuordnen, derart dass der Grad von $g(\varpi)$ mit der Ordnung der Gruppe G von $f(z) = 0$ übereinstimmt. Sind durch gewisse Adjunctionen alle Wurzeln von $f = 0$ bekannt, so zerfällt $g(\varpi)$ in lineare, rational bekannte Factoren.

§ 569. Von den im vorigen Paragraphen besprochenen Gleichungen gelangen wir zu den Abel'schen Gleichungen, wenn wir zu den bisher zu Grunde gelegten Relationen unter den Wurzeln

$$z_1,\quad z_2 = \varphi_2(z_1),\quad z_3 = \varphi_3(z_1),\quad \cdots\quad z_n = \varphi_n(z_1)$$

noch die Bedingungen der Vertauschbarkeit

$$\varphi_i(\varphi_k(z_1)) = \varphi_k(\varphi_i(z_1))$$

für alle Combinationen i, k hinzunehmen. Es fragt sich, welchen Einfluss diese neuen Bedingungen auf die Gruppe der Gleichung ausüben werden.

Ist s_1 diejenige Substitution von G, welche z_1 in $z_a = \varphi_a(z_1)$ umwandelt, so führt sie jedes $z_b = \varphi_b(z_1)$ in $\varphi_b(z_a) = \varphi_b(\varphi_a(z_1))$ über.

Ist s_2 diejenige Substitution von G, welche z_1 in z_b umwandelt, so führt sie $z_a = \varphi_a(z_1)$ in $\varphi_a(z_b) = \varphi_a(\varphi_b(z_1))$ über.

Es führt also $s_1 s_2$ die Wurzel

$$z_1 \quad \text{in} \quad \varphi_a(\varphi_b(z_1)),$$

und $s_2 s_1$ die Wurzel

$$z_1 \quad \text{in} \quad \varphi_b(\varphi_a(z_1)) = \varphi_a(\varphi_b(z_1))$$

über. Da Gleiches von allen Wurzeln und allen Substitutionen gilt, so ist die Gruppe einer Abel'schen Gleichung G eine transitive, reguläre Gruppe vertauschbarer Substitutionen.

Betrachten wir nun umgekehrt eine Gruppe der eben bezeichneten Art, deren Substitutionen also unter einander vertauschbar sein sollen, dann kann man die Schlüsse einfach umkehren. Es führt die Anwendung von $s_1 s_2$ das Element z_1 in $\varphi_a(\varphi_b(z_1))$ über, und $s_2 s_1$ führt dasselbe Element z_1 nach $\varphi_b(\varphi_a(z_1))$. Da nun $s_1 s_2 = s_2 s_1$ sein soll, so muss sich ergeben, was auch a und b sein mögen,

$$\varphi_a(\varphi_b(z_1)) = \varphi_b(\varphi_a(z_1)); \tag{5}$$

folglich haben wir es wieder mit einer irreductiblen Abel'schen Gleichung zu thun.

Nun hatten wir in § 503 die Voraussetzung der Irreductibilität bei Seite gelassen. Genau das Gleiche können wir hier thun. Ist die Gruppe einer Gleichung nämlich intransitiv, und sind ihre Substitutionen regulär und vertauschbar unter einander, dann werden nach Adjunction einer Wurzel sämmtliche Wurzeln bekannt sein, und ebenso folgt wie bisher (5). Es kommt nur die Irreductibilität von $f(z)$ in Wegfall. Die Ordnung der Gruppe wird kleiner als der Grad von f.

Wir können eine weitere Specialisirung dadurch eintreten lassen, dass wir statt der allgemeinen irreductiblen Abel'schen Gleichung eine cyklische Gleichung betrachten, d. h. eine irreductible Abel'sche, deren Wurzeln in einen einzigen Cyklus iterirter Functionen eingeordnet werden können. Deuten wir die Ordnung der Iterirung durch obere Indices an, so wird die Reihe der Wurzeln durch

$$z_1, \ \Theta(z_1), \ \Theta^{(2)}(z_1), \ \cdots \ \Theta^{(n-1)}(z_1)$$

gegeben. Bezeichnen wir nun diejenige Substitution der Gruppe, welche z_1 in $\Theta(z_1)$ überführt, mit s, so sieht man sofort, dass diejenige, welche z_1 in $\Theta^2(z_1)$ umwandelt, gleich s^2 sein muss, u. s. f. Daraus folgt: Die Gruppe einer cyklischen Gleichung ist cyklisch, und umgekehrt.

§ 570. Wir wollen uns mit einer gruppentheoretischen Eigenschaft der transitiven Gruppen etwas eingehender beschäftigen.

Wir haben eine transitive Gruppe als solche definirt, die auf z_1 jedes andere Element $z_1, z_2, \cdots z_n$ folgen lässt. Daraus ergiebt sich, dass sie Substitutionen besitzt, die jedes beliebige z_α in jedes beliebige z_β überführen. Denn wenn s_α auf z_1 folgen lässt z_α, und wenn s_β auf z_1 folgen lässt z_β, dann bewirkt die Substitution $s_\alpha^{-1} s_\beta$, welche ja ebenfalls in der Gruppe vorkommt, dass z_β auf z_α folgt. Demnach können wir die Definition auch so fassen, dass man durch geeignete Substitutionen einer transitiven Gruppe auf ein beliebiges Element z_α alle anderen Elemente folgen lassen kann.

Aus der transitiven Gruppe G greifen wir zunächst diejenigen Substitutionen

$$t_1 = 1, \; t_2, \; t_3, \; \cdots \; t_q \tag{6}$$

heraus, welche z_1 nicht umsetzen. Diese bilden einen Theiler T von G. Ferner sei s_2 eine der Substitutionen, welche z_2 auf z_1 folgen lassen. Dann werden

$$s_2, \; t_2 s_2, \; t_3 s_2, \; \cdots \; t_q s_2 \tag{7}$$

sämmtlich das Gleiche thun, wie sofort zu sehen ist, und nur sie. Denn zuerst führt t_α das Element z_1 in sich selbst, und s_2 führt es in z_2 über. — Wenn andrerseits die Substitution τ gleichfalls die Folge $z_1 z_2$ enthielte, dann würde τs_2^{-1} zu (6) gehören, und aus der dies ausdrückenden Gleichung

$$\tau s_2^{-1} = t_\alpha \quad \text{folgt} \quad \tau = t_\alpha s_2.$$

Ist die Gruppe G durch (6) und (7) noch nicht erschöpft, d. h. ist $n > 2$, dann gehen wir in der gleichen Weise weiter, indem wir irgend ein s_3 zu Grunde legen, welches z_3 auf z_1 folgen lässt und mit ihm entsprechend (7) die Reihe

$$s_3, \; t_2 s_3, \; t_3 s_3, \; \cdots \; t_q s_3 \tag{8}$$

bilden. So geht man bis zu einem s_n, welches die Folge $z_1 z_n$ enthält. Hieraus ist ersichtlich: Die Ordnung r einer transitiven Gruppe G von n Elementen ist durch n theilbar, so dass $r = n \cdot q$ gesetzt werden kann. Dabei bedeutet q die Ordnung desjenigen Theilers von G, dessen Substitutionen eins der Elemente ungeändert lassen.

§ 571. Wir nennen eine Gruppe zweifach transitiv, wenn wir mit Hülfe ihrer Substitutionen zwei Elemente z_1 und z_2 an zwei willkürlich vorgeschriebene Plätze z_α und z_β bringen können. Daraus

folgt zunächst, dass man überhaupt zwei willkürliche Elemente z_λ, z_μ durch zwei willkürliche z_α, z_β ersetzen kann. Denn, wenn s_1 auf z_1, z_2 folgen lässt z_λ, z_μ, und wenn s_2 auf z_1, z_2 folgen lässt z_α, z_β, so wird $s_1^{-1}s_2$ das Gewünschte leisten.

Wir können nun ähnliche Schlussfolgerungen machen wie die im vorigen Paragraphen durchgeführten, indem wir die Gesammtheit der Substitution der Reihe (6) als denjenigen Theiler auffassen, dessen Substitutionen weder z_1 noch z_2 umstellen; dann wird (7) der Complex der Substitutionen, welche eine und dieselbe Aenderung mit z_1 und z_2 vornehmen, u. s. f. Daraus folgt: Die Ordnung r einer zweifach transitiven Gruppe G von n Elementen ist durch $\binom{n}{2}$ theilbar, so dass $r = \binom{n}{2} q$ gesetzt werden kann. Dabei bedeutet q die Ordnung desjenigen Theilers von G, dessen Substitutionen zwei der Elemente ungeändert lassen. Die Minimalordnung einer solchen Gruppe ist also $\frac{1}{2} n(n-1)$.

Für $n = 5$ hat man beispielsweise die Gruppe

$$\begin{array}{llll}
1\quad, & (z_2z_3z_5z_4), & (z_2z_5)(z_3z_4), & (z_2z_4z_5z_3), \\
(z_1z_2z_3z_4z_5), & (z_1z_2z_4z_3), & (z_1z_2)(z_3z_5), & (z_1z_2z_5z_4), \\
(z_1z_3z_5z_2z_4), & (z_1z_3z_2z_5), & (z_1z_3)(z_4z_5), & (z_1z_3z_4z_2), \\
(z_1z_4z_2z_5z_3), & (z_1z_4z_5z_2), & (z_1z_4)(z_2z_3), & (z_1z_4z_3z_5), \\
(z_1z_5z_4z_3z_2), & (z_1z_5z_3z_4), & (z_1z_5)(z_2z_4), & (z_1z_5z_2z_3).
\end{array}$$

Besitzt eine Gleichung $f(z) = 0$ eine zweifach transitive Gruppe G, dann ist dies charakteristisch dafür, dass man in jeder rationalen Relation

$$g(z_1, z_2, z_3, \cdots z_n) = 0$$

zwei beliebige der Wurzeln, z. B. z_1, z_2, durch zwei beliebige andere ersetzen kann, während dabei die übrigen Wurzeln $z_3, \cdots z_n$ in gewisse neue übergehen; man hat also auch

$$g(z_\alpha, z_\beta, z_{i_3}, \cdots z_{i_n}) = 0,$$

wobei α, β beliebig gewählt werden konnten. —

Ist z. B. die Gleichung $f(z) = 0$ mit zweifach transitiver Gruppe so beschaffen, dass alle ihre Wurzeln durch zwei unter ihnen, z_1 und z_2, rational darstellbar sind, etwa in der Form

$$(6) \qquad z_3 = \varphi_3(z_1, z_2), \quad z_4 = \varphi_4(z_1, z_2), \quad \cdots \quad z_n = \varphi_n(z_1, z_2),$$

dann hat man auch für beliebige α, β

$$(7) \qquad z_{i_3} = \varphi_3(z_\alpha, z_\beta), \quad z_{i_4} = \varphi_4(z_\alpha, z_\beta), \quad \cdots \quad z_{i_n} = \varphi_n(z_\alpha, z_\beta).$$

Die $z_{i_3}, z_{i_4}, \cdots z_{i_n}$ sind hier von einander verschieden, weil aus

$$\varphi_\varkappa(z_\alpha, z_\beta) = \varphi_\lambda(z_\alpha, z_\beta) \quad \text{folgt} \quad \varphi_\varkappa(z_1, z_2) = \varphi_\lambda(z_1, z_2);$$

ebenso sind sie von z_α oder z_β selbst aus demselben Grunde verschieden. Folglich giebt (7) alle Wurzeln mit Ausnahme von z_α, z_β; d. h. alle Wurzeln sind rational durch zwei beliebige unter ihnen darstellbar.

Findet nun eine solche Darstellung statt, dann ist nach Adjunction zweier beliebiger Wurzeln z_α und z_β die Gleichung aufgelöst; die Gruppe reducirt sich dabei auf 1. Folglich enthielt sie vorher nur solche Substitutionen, welche alle n Elemente, oder nur $(n-1)$ oder gar kein Element umsetzen. Die Umkehrung dieses Satzes ist, wie man leicht sieht, gleichfalls richtig.

§ 572. Um die Natur derartiger Gruppen, welche nur $n, n-1$ oder 0 Elemente umsetzen, genauer zu erforschen, wollen wir folgenden Satz herleiten*): In jeder transitiven Gruppe G des Grades n giebt es mindestens $(n-1)$ Substitutionen, welche alle n Elemente umsetzen. Giebt es mehr als $(n-1)$ derartige Substitutionen in G, so besitzt die Gruppe auch solche Substitutionen, welche weniger als $(n-1)$ Elemente umsetzen.

Wir bezeichnen denjenigen Theiler von G, welcher das Element z_α nicht ändert, mit G_α, und eine derjenigen Substitutionen, welche z_1 in z_α überführen, mit σ_α. Dann ist

$$G_1 = \sigma_2 G_2 \sigma_2^{-1} = \sigma_3 G_3 \sigma_3^{-1} = \cdots = \sigma_n G_n \sigma_n^{-1},$$

d. h. alle diese Gruppen G_α sind einander ähnlich. Nun möge m ihre gemeinsame Ordnung sein, und $[q]$ die Zahl derjenigen Substitutionen von G_1 und also auch von $G_2, \cdots G_n$, welche genau q und nur q Elemente umstellen. Diesen Definitionen gemäss haben wir

$$m = [n-1] + [n-2] + \cdots + [q] + \cdots + [0].$$

Natürlich hat $[0]$ den Werth 1, da es sich allein auf die identische Substitution bezieht.

In allen G_α $(\alpha = 1, 2, \cdots n)$ zusammen kommen $n \cdot [n-1]$ Substitutionen vor, welche $(n-1)$ Elemente umsetzen, und diese sind unter einander verschieden, da keine Substitution aus G_α, die nur z_α nicht umsetzt, auch in G_β enthalten ist.

In allen G_α zusammen kommen $n \cdot [n-2]$ Substitutionen vor, welche genau $(n-2)$ Elemente umsetzen; aber diese sind zu je zwei

*) C. Jordan, Journ. de Math. (2), 17, p. 351.

und zwei identisch, da diejenigen Substitutionen, welche in G_α das Element z_β nicht umsetzen, dieselben sind wie diejenigen, welche in G_β das Element z_α nicht umsetzen. Es giebt also von diesen Substitutionen $\frac{1}{2} n \cdot [n-2]$.

Ebenso kommen in allen G_α zusammen $\frac{1}{3} n \cdot [n-3]$ von einander verschiedene Substitutionen vor, welche genau $(n-3)$ Elemente umstellen, u. s. w.

Somit ist die Anzahl aller Substitutionen in G, welche weniger als n Elemente umstellen, gleich

$$\frac{n}{1}[n-1] + \frac{n}{2}[n-2] + \cdots + \frac{n}{n-q}[q] + \cdots + 1[0].$$

Diese Zahl wollen wir von derjenigen aller Substitutionen in G d. h. nach § 570, Schluss, von mn abziehen. Benutzen wir den obigen Werth für m, so findet sich für jene Differenz

$$n\left(\frac{1}{2}[n-2] + \frac{2}{3}[n-3] + \cdots + \frac{n-q-1}{n-q}[q] + \cdots + \frac{n-1}{n}[0]\right);$$

dies ist somit die Anzahl aller derjenigen Substitutionen aus G, welche sämmtliche Elemente umstellen. Jeder der einzelnen Summanden in der Klammer ist positiv oder Null. Der letzte ist sicher positiv, nämlich $= \frac{n-1}{n}$. Folglich hat jene Differenz einen positiven Werth, der nicht unter $(n-1)$ sinken kann. Ist der Werth grösser als $(n-1)$, so ist mindestens eines der Symbole $[q]$ von Null verschieden, wobei q nicht grösser als $(n-2)$ werden kann.

Damit ist der ausgesprochene Satz in allen Theilen bewiesen.

Wenden wir ihn auf die im vorigen Paragraphen besprochenen Verhältnisse an, so sehen wir, dass eine transitive Gruppe G, welche nur Substitutionen von n und von $(n-1)$ Elementen neben der Einheit besitzt, genau $(n-1)$ Substitutionen haben wird, welche alle Elemente umsetzen.

Auch über die Anzahl derjenigen Substitutionen von G, welche genau $(n-1)$ Elemente umsetzen, können wir Aufklärung erhalten, wenn wir bedenken, dass in G_1 nicht zwei Substitutionen s_μ, s_ν vorkommen dürfen, die eine gleiche Elementenfolge darbieten, weil sonst $s_\mu s_\nu^{-1}$ weniger Elemente umsetzen würde, ohne $=1$ zu sein. Nun giebt es zwischen $z_2, z_3, \cdots z_n$ nur $(n-1)(n-2)$ Folgen z_α, z_β, und jede Substitution aus G_1 enthält deren $(n-1)$; folglich kann G_1 höchstens $(n-2)$ solcher Substitutionen besitzen, und in G kommen höchstens $n(n-2)$ vor, welche genau ein Element nicht ändern.

Demnach kann die Ordnung der Gruppe die Zahl

$$(n-1)+n(n-2)+1=n(n-1)$$

nicht übertreffen. —

Auf dem in den letzten Paragraphen beschrittenen Wege kann man zum Begriffe drei- und mehrfacher Transitivität gelangen.

§ 573. Wir wollen noch eine Anwendung der eingeführten Begriffe geben. Ist $f(z)=0$ eine irreductible Gleichung n^{ten} Grades mit der Galois'schen Gruppe G, so sei H ein Theiler von G. Dabei mögen H und G die Ordnungen r_1 und $r=r_1q$ besitzen. Eine zu H gehörige Function $\varphi(z_1, z_2, \cdots z_n)=\varphi_1$ möge durch die Substitutionen von G die Werthe

$$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_q$$

annehmen, und $\sigma_1=1, \sigma_2, \sigma_3, \cdots \sigma_q$ seien Substitutionen aus G, welche φ_1 in diese verschiedenen conjugen Werthe umwandelt.

Wir haben im § 540 gezeigt, dass $\varphi_1, \varphi_2, \cdots \varphi_q$ Wurzeln einer Gleichung sind, deren Coefficienten zu dem Rationalitätsbereiche von $f(z)$ gehören. Hier soll nun die Irreductibilität dieser Gleichung nachgewiesen werden; und damit ist natürlich auch die Irreductibilität der in § 540; I abgeleiteten Gleichung ϱ^{ten} Grades gezeigt.

Gesetzt, die Gleichung q^{ten} Grades zerfalle, und $\varphi_1, \varphi_2, \cdots \varphi_p$ $(p<q)$ seien die Wurzeln einer der irreductiblen Factorengleichungen. Dann sind die symmetrischen Functionen von $\varphi_1, \varphi_2, \cdots \varphi_p$ bekannt, und so bleibt z. B.

$$\varphi_1^u+\varphi_2^u+\cdots+\varphi_p^u \tag{8}$$

für alle Substitutionen der Gruppe G ungeändert, wie auch u ganzzahlig gewählt werden mag. Wir wählen es so, dass aus einer Relation

$$\varphi_{i_1}^u+\varphi_{i_2}^u+\cdots=\varphi_{k_1}^u+\varphi_{k_2}^u+\cdots$$

die Gleichheit der einzelnen Summanden links und rechts folgt (§ 539). Nun wenden wir auf (8) die Substitution σ_{p+1} aus G an. Diese führt φ_1 in φ_{p+1} über. Folglich kann (8) für die Gruppe der Gleichung nicht ungeändert bleiben. Das ist ein Widerspruch, der nur durch $p=q$ gehoben wird, d. h.: Die Gleichung, von welcher φ abhängt, ist irreductibel.

§ 574. Die bisher in dieser Vorlesung durchgeführten Untersuchungen hatten in dem Begriffe der Reductibilität oder der Irreductibilität einer Gleichung ihren Ausgangspunkt. Wir wollen jetzt in ähnlicher Art die Primitivität oder die Imprimitivität von Gleichungen untersuchen.

Im § 491 kamen wir auf irreductible Gleichungen $f(z) = 0$, deren Polynom $f(z)$ in folgender Weise ausgedrückt werden konnte:

$$(9) \qquad f(z) = h(z; y_1) \cdot h(z; y_2) \cdots h(z; y_\mu); \qquad (n = \mu \cdot m),$$

$$(10) \quad h(z; y_\alpha) = z^m - \gamma_1(y_\alpha) z^{m-1} + \gamma_2(y_\alpha) z^{m-2} - \cdots \pm \gamma_m(y_\alpha),$$

wobei die γ rationale ganze Functionen des Argumentes y_α waren, und die y_α Wurzeln einer Gleichung μ^{ten} Grades bedeuteten,

$$(11) \qquad g(y) \equiv y^\mu - d_1 y^{\mu-1} + d_2 y^{\mu-2} - \cdots \pm d_\mu = 0.$$

Es wird dabei also $f(z) = 0$ die Eliminante von $h(z; y) = 0$ und $g(y) = 0$. Nach der Auflösung von (11) und Adjungirung aller ihrer Wurzeln zerfällt $f(z)$ in μ Factoren des Grades m.

Wir werfen die Frage auf, wie diese Eigenschaft von $f(z) = 0$ sich bei der Galois'schen Gruppe der Gleichung kenntlich macht.

Wir wollen die Wurzeln von

$$h(z; y_\alpha) = 0 \quad \text{mit} \quad z_{\alpha 1}, z_{\alpha 2}, \cdots z_{\alpha m} \qquad (\alpha = 1, 2, \cdots \mu)$$

bezeichnen. Nun sind durch die Adjunction von y_α die symmetrischen Functionen der $z_{\alpha 1}, z_{\alpha 2}, \cdots z_{\alpha m}$ bekannt. Es sei $S(z_{\alpha 1}, \cdots z_{\alpha m})$ eine solche; dann sind die Werthe, die S annehmen kann, Wurzeln einer irreductiblen Gleichung (§ 573). Drückt man $S(z_{\alpha 1}, \cdots z_{\alpha m})$ als Function von y_α aus, dann zeigt (11), dass der Grad dieser Gleichung nicht höher werden kann als μ. Andrerseits giebt es wirklich μ Werthe

$$(12) \qquad S(z_{11}, \cdots z_{1m}), \; S(z_{21}, \cdots z_{2m}), \; \cdots \; S(z_{\mu 1}, \cdots z_{\mu m});$$

dies sind mithin die einzigen, welche S für die Substitutionen der Gruppe G von $f(z) = 0$ annehmen kann.

Wenden wir somit eine Substitution s von G auf die Reihe (12) an, so kann sie nur in sich selbst übergehen abgesehen von der Aufeinanderfolge der Functionen. Führt also ein $s_\varkappa$ eins der Elemente von $z_{\alpha 1}, \cdots z_{\alpha m}$ in eins derjenigen von $z_{\beta 1}, \cdots z_{\beta m}$ über, dann muss der ganze Complex jener Elemente in denjenigen dieser Elemente umgewandelt werden. Lässt insbesondere $s_\varkappa$ ein $z_{\beta\gamma}$ ungeändert, dann gehen die übrigen $z_{\beta 1}, \cdots z_{\beta m}$ nur unter einander Vertauschungen ein. G versetzt also nur die Serien der in (12) angeordneten Elemente unter sich und weiter auch in jeder einzelnen Serie die zugehörigen Elemente unter einander.

Eine derartige Gruppe heisst eine imprimitive; ebenso heisst die zugehörige Gattung imprimitiv, und ebenso die Gleichung, deren Galois'sche Gattung imprimitiv ist. Hat eine Gruppe diese Eigenschaft nicht, so heisst sie primitiv; das Gleiche gilt von der Gattung und von der Gleichung.

Es ist z. B. die Gruppe, welche aus den Potenzen der Substitution

$$s = (z_1 z_2 z_3 z_4 z_5 z_6)$$

besteht, imprimitiv. Die Eintheilung der Elemente kann in die Serien

$$z_1,\ z_3,\ z_5 \quad \text{und} \quad z_2,\ z_4,\ z_6$$

geschehen, aber ebenso gut auch in die Serien

$$z_1,\ z_4;\quad z_2,\ z_5;\quad z_3,\ z_6. \text{ —}$$

Wenn umgekehrt die Gruppe G einer Gleichung $f(z) = 0$ imprimitiv ist, und wenn

$$z_{\alpha 1},\ z_{\alpha 2},\ \cdots\ z_{\alpha m} \qquad (\alpha = 1, 2, \cdots \mu)$$

die Eintheilung der Wurzeln in die Systeme der Imprimitivität angiebt, dann sei $S(z_{\alpha 1}, \cdots z_{\alpha m})$ irgend eine symmetrische Function. Durch (12) werden dann wegen der Imprimitivität alle Werthe gegeben, die $S(z_{11}, \cdots z_{1m})$ im Rationalitätsbereiche annehmen kann; die symmetrischen Functionen der Grössen (12) sind also rational bekannt, und sie selbst genügen einer Gleichung

$$(13) \qquad S^\mu - D_1 S^{\mu-1} + D_2 S^{\mu-2} - \cdots \pm D_\mu = 0$$

mit rational bekannten Coefficienten D. Weiter lässt sich jede andere symmetrische Function von $z_{\alpha 1}, \cdots z_{\alpha m}$ durch $S(z_{\alpha 1}, \cdots z_{\alpha m})$ im Rationalitätsbereiche darstellen; folglich kann man setzen

$$f(z) = h(z; S_1) \cdot h(z; S_2) \cdots h(z; S_\mu),$$

wo die S die Wurzeln der Gleichung (13) und die

$$h(z; S_\alpha) = (z - z_{\alpha 1}) \cdots (z - z_{\alpha m})$$

sind.

Demnach ist $f(z) = 0$ das Eliminationsresultat von S aus (13) und aus $h(z; S) = 0$, und wir können sagen: Dafür dass eine Gleichung $f(z) = 0$ das Eliminationsresultat von $h(z; y) = 0$ und $g(y) = 0$ wird, ist es charakteristisch, dass die Galois'sche Gruppe von $f = 0$ imprimitiv sei.

§ 575. Wir betrachten denjenigen Theiler H der imprimitiven Gruppe G des vorigen Paragraphen, dessen Substitutionen nur die Elemente jedes einzelnen Imprimitivitätssystems unter sich vertauschen. Diese Gruppe ist ein autojuger Theiler in G. Denn wenn σ_α auf H zur Transformirung verwendet wird, so gehen dadurch z. B. die Elemente $z_{\varkappa 1}, \cdots z_{\varkappa m}$ in $z_{\lambda 1}, \cdots z_{\lambda m}$ über; und wenn H die Systeme nicht vertauschte, so kann auch $\sigma_\alpha^{-1} H \sigma_\alpha$ es nicht thun.

Ist also H von der Einheit verschieden, dann ist G zusammengesetzt.

Beim Beispiele des vorigen Paragraphen giebt es Substitutionen, welche die Systeme nicht ändern; deswegen ist auch jene Gruppe zusammengesetzt; im Falle der ersten Systemeintheilung sind s^2 und s^4 diese Substitutionen; im Falle der zweiten ist es s^3.

Umgekehrt erkennt man leicht: Hat eine zusammengesetzte Gruppe G einen intransitiven, autojugen Theiler, dann ist G imprimitiv.

Neunundfünfzigste Vorlesung.

Resolventen.

§ 576. Wir hatten einer Gleichung $f(z) = 0$ mit der Gruppe G eine rationale ganze Function der n Wurzeln $h(z_1, z_2, \cdots z_n)$ adjungirt, d. h. h im Bereiche G als bekannt angesehen. Eine solche adjungirte Function wird häufig als Resolvente bezeichnet, und wir haben diese Bezeichnung schon gelegentlich bei der Einführung der Lagrange'schen Resolvente (Bd. I, § 320) benutzt.

Hiernach ist jede beliebige ganze Function der Wurzeln geeignet als Resolvente zu fungiren. Von Vortheil können aber nur diejenigen Functionen für die Lösung der Gleichung werden, welche nicht schon dem Rationalitätsbereiche angehören; so ist es z. B. zwecklos, einer allgemeinen Gleichung eine symmetrische Function zu adjungiren.

Die Wirkung einer Adjunction von $h(z_1, \cdots z_n)$ beruht nämlich darauf, die Gruppe G auf die desjenigen ihrer Theiler zu reduciren, welcher $h(z_1, \cdots z_n)$ ungeändert lässt. Es reicht daher stets aus, h so zu wählen, dass die zugehörige Gruppe H ein Theiler von G ist.

Bedeutet G die symmetrische Gruppe, so können wir einige für jedes n vorhandene Resolventen, oder besser Resolventengattungen anführen; denn nach dem Dargelegten kommt es nicht auf das Individuum h, sondern nur auf die Gruppe H an. Zu diesen Resolventen gehören die zweiwerthigen, insbesondere die alternirenden Functionen, welche durch die Quadratwurzel aus der Discriminante charakterisirt sind. Ist $n > 4$, dann giebt es keine Resolventen, deren Werthezahl $\varrho < n$ ist. Für $\varrho = n$ haben wir die durch $h = z_1$ charakterisirte Gattung; ihre Gruppe H besteht aus allen Substitutionen, durch welche eins der Elemente nicht umgesetzt wird. Für $n = 6$ giebt es daneben gemäss § 547 noch eine durch

$$h(z_1, \cdots z_6) = (z_1 z_2 + z_3 z_4 + z_5 z_6)(z_1 z_3 + z_2 z_5 + z_4 z_6)(z_1 z_4 + z_2 z_6 + z_3 z_5)$$
$$(z_1 z_5 + z_2 z_4 + z_3 z_6)(z_1 z_6 + z_2 z_3 + z_4 z_5)$$

charakterisirte Gattung. Von der grössten Wichtigkeit ist die Galoissche Gattung, zu der Resolventen mit $\varrho = n!$ Werthen gehören,

$$\varpi = u_1 z_1 + u_2 z_2 + \cdots + u_n z_n.$$

§ 577. Wir wissen bereits, dass eine solche Resolvente $h(z_1, \cdots z_n)$ mit ϱ Werthen die Wurzel einer Gleichung ϱ^{ten} Grades ist, deren Coefficienten dem Rationalitätsbereiche angehören. Die Gleichung ist irreductibel (§ 573).

Die Adjungirung von h ist also identisch mit der Annahme, dass eine Wurzel dieser Resolventengleichung bekannt sei, oder dass man eine solche bestimmen könne, falls gewisse Hülfsmittel zugelassen werden. Man könnte also z. B. die Ausziehung einer Wurzel aus einer bekannten Grösse als erlaubte Operation ansehen; wenn jetzt eine Resolventengleichung binomisch wird, dann müsste die zugehörige Function $h(z_1, \cdots z_n)$ als bekannt gelten.

Die Thatsache allein, dass die Resolventengleichung den Grad ϱ besitzt und irreductibel ist, reicht für die Einsicht in ihre Natur noch nicht hin. Wir wollen, um diese genauer zu erkennen, die Gruppe der Resolventengleichung aufsuchen.

Es sei der Gleichung $f(z) = 0$ mit den Wurzeln $z_1, z_2, \cdots z_n$ und der Gruppe G die Resolvente $h(z_1, z_2, \cdots z_n) = h_1$ adjungirt, welche zur Gruppe H gehören möge; die übrigen Werthe in dem durch G bestimmten Rationalitätsbereiche seien $h_2, h_3, \cdots h_\varrho$, und

$$(1) \quad (\eta - h_1)(\eta - h_2) \cdots (\eta - h_\varrho) = \eta^\varrho - A_1 \eta^{\varrho-1} + A_2 \eta^{\varrho-2} - \cdots = 0$$

sei die Resolventengleichung. Ihre Gruppe H_0 hat die Eigenschaft, dass alle und nur diejenigen Functionen von $h_1, h_2, \cdots h_\varrho$, welche unter dem Einflusse der Substitutionen von H_0 ungeändert bleiben, rational durch die A, d. h. also auch durch die Coefficienten von $f(z)$ darstellbar sind.

Zu dem Zwecke der Feststellung dieser Gruppe wenden wir auf die Reihe der in G conjugen Werthe von h, nämlich

$$(2) \qquad h_1, h_2, \cdots h_\varrho$$

die sämmtlichen Substitutionen s von G an; durch eine solche s_i geht (2) bis auf die Reihenfolge in sich selbst über; denn (2) umfasst eben alle Werthe, die h_1 überhaupt unter dem Einflusse der Substitutionen von G annehmen kann. Die neue Reihe der Werthe h wollen wir mit

$$(3) \qquad h_{i_1}, h_{i_2}, \cdots h_{i_\varrho}$$

bezeichnen; dann lässt sich der Uebergang von (2) auf (3) als eine

Substitution (§ 518) auffassen, die wir entsprechend früheren Festsetzungen bezeichnen

$$t_i = \binom{h_\varkappa}{h_{i_\varkappa}} \qquad (\varkappa = 1, 2, \cdots \varrho).$$

Ist s_j eine zweite Substitution aus G, und bedeutet in gleicher Weise

$$t_j = \binom{h_\varkappa}{h_{j_\varkappa}} \qquad (\varkappa = 1, 2, \cdots \varrho)$$

die entsprechende Substitution unter den h, dann erkennt man, dass dem Producte $s_i s_j$ entsprechen wird

$$t_i t_j = \binom{h_\varkappa}{h_{i_\varkappa}} \binom{h_{i_\varkappa}}{h_{j_{i_\varkappa}}} = \binom{h_\varkappa}{h_{j_{i_\varkappa}}} \qquad (\varkappa = 1, 2, \cdots \varrho),$$

und daraus schliesst man, dass die $t_1, t_2, \cdots$ sämmtlich eine Gruppe bilden; diese wollen wir mit H_0 bezeichnen.

Ferner sieht man, dass wenn G die symmetrische Gruppe der n Elemente z_λ ist, dann G und H_0 im Allgemeinen einstufig isomorph zu einander sind. Denn jedem s_α entspricht ein t_α; wenn ferner aber einem t_α sowohl s_α als s'_α entspräche, dann würde dem $s'_\alpha s_\alpha^{-1}$ entsprechen $t_\alpha t_\alpha^{-1} = 1$, d. h. die Substitution $s'_\alpha s_\alpha^{-1}$ würde in (2) keine Aenderung der Folge hervorrufen, was nach § 543 nur bei $\varrho = 1$, bei $\varrho = 2$ und bei gewissen Gruppen von vier Elementen vorkommen kann. Es ist deswegen H_0 im allgemeinen Falle von derselben Ordnung wie G, bei allgemeinen Gleichungen also von der Ordnung $n!$.

Der Compositionsreihe von G entspricht diejenige von H_0, und die Compositionsfactoren sind für beide Gruppen dieselben.

Wir fragen nun, wann eine Function der $h_1, \cdots h_\varrho$

$$\psi(h_1, h_2, \cdots h_\varrho) = \chi(z_1, z_2, \cdots z_n)$$

rational bekannt ist? Da ψ als Function der $z_1, z_2, \cdots$ dargestellt werden kann $= \chi$, so ist es charakteristisch dafür, dass χ für G ungeändert bleibt. Den Substitutionen von G entsprechen die von H_0; demnach muss ψ zu H_0 gehören. Wenn umgekehrt ψ zu H_0 gehört, so wird χ zu G gehören, und somit ist $\psi = \chi$ rational bekannt.

Folglich ist H_0 die zur Resolventengleichung (1) gehörige Gruppe.

Der Definition nach giebt es Substitutionen von G, welche jedes Element in (2) auf h_1 folgen lassen; es kommen daher in H_0 alle Folgen $h_1 h_2$; $h_1 h_3$; $\cdots h_1 h_\varrho$ vor; d. h. die Gruppe H_0 ist, wie früher schon auf andere Art bewiesen wurde (§ 573), transitiv.

Aus dem abgeleiteten Theoreme kann man noch einen für die Theorie der Abel'schen Gleichungen wichtigen Satz ablesen. Sind $z_1, z_2, \cdots z_n$ die n Wurzeln einer Abel'schen Gleichung $f(z) = 0$, so betrachten wir eine Resolvente $h(z_1, \cdots z_n)$, die wegen der charakteristischen Eigenschaft der Abel'schen Gleichungen auch

$$h(z_1, z_2, \cdots z_n) = h(z_1, \varphi_2(z_1), \cdots \varphi_n(z_1)) = k(z_1)$$

geschrieben werden kann. Hieraus ergiebt sich die Gruppe der zu $h(z_1, \cdots z_n)$ gehörigen Resolventengleichung. Es hat nämlich h nur ϱ Werthe

$$k(z_1),\ k(z_2),\ \cdots\ k(z_\varrho).$$

Wendet man die Gruppe der Abel'schen Gleichung auf diese Reihe an, die man auch

$$k(z_1),\ k(\varphi_2(z_1)),\ \cdots\ k(\varphi_\varrho(z_1))$$

setzen kann, so erkennt man aus den Betrachtungen des vorigen Paragraphen über t_i und t_j, dass mit den Substitutionen der s von G zugleich die unter den k hervorgerufenen Substitutionen vertauschbar sind. Jede rationale Function der Wurzeln einer Abel'schen Gleichung ist wiederum Wurzel einer Abel'schen Gleichung.

Ebenso ergiebt sich, dass jede rationale Function der Wurzeln einer cyklischen Gleichung wiederum Wurzel einer cyklischen Gleichung wird.

§ 578. Es sei G eine beliebige Gruppe, und die adjungirte Function $h(z_1, \cdots z_n) = h_1$ gehöre zu einem autojugen Theiler H von G. Wendet man nun auf die Reihe (2) eine Substitution σ aus H an, so wird sich h_1 dabei nicht ändern. Gleichzeitig werden mit h_1 alle h_i ungeändert bleiben. Denn setzt s_i das Element h_i an die Stelle von h_1, so gehört zu h_i dieselbe Gruppe

$$s_i^{-1} H s_i = H,$$

weil H autojug in G ist. Also bleibt (2) für alle Substitutionen σ aus H auch der Reihenfolge nach ungeändert.

Allgemeiner kann man sagen, dass zwei Substitutionen s und s_1 dieselbe Umstellung von (2) und also eine gleiche Substitution der h_α bewirken, wenn $s_1 = \sigma s$ ist, wobei σ der Gruppe H angehört.

Besitzt H die Ordnung q, G die Ordnung r, und ist $r = q \cdot m$, dann gehören je q Substitutionen von G zu einer Substitution von H_0. Diese Gruppe H_0 der Resolventengleichung besitzt die Ordnung m, und G ist zu ihr q-stufig isomorph.

Wählen wir z. B. für G die symmetrische Gruppe der vier Elemente z_1, z_2, z_3, z_4 und für H die autojuge Gruppe

$$H = [1,\ (z_1 z_2)(z_3 z_4),\ (z_1 z_3)(z_2 z_4),\ (z_1 z_4)(z_2 z_3)],$$

setzen wir ferner

$$\begin{array}{lll} h_1 = \quad (z_1 - z_2)(z_3 - z_4), & h_3 = \quad (z_1 - z_3)(z_2 - z_4), & h_5 = \quad (z_1 - z_4)(z_2 - z_3); \\ h_2 = -(z_1 - z_2)(z_3 - z_4), & h_4 = -(z_1 - z_3)(z_2 - z_4), & h_6 = -(z_1 - z_4)(z_2 - z_3), \end{array}$$

dann erhalten wir als Gruppe H_0 eine Gruppe der Ordnung 6, zu welcher G vierstufig isomorph wird. Es ist dies die Gruppe, welche aus

$$1,\ (h_1 h_2)(h_3 h_5)(h_4 h_6),\ (h_1 h_3)(h_2 h_4)(h_5 h_6),\ (h_1 h_4 h_5)(h_2 h_3 h_6),$$
$$(h_1 h_5 h_4)(h_2 h_6 h_3),\ (h_1 h_6)(h_2 h_5)(h_3 h_4)$$

besteht. Jeder ihrer Substitutionen entsprechen vier Substitutionen der symmetrischen Gruppe; insbesondere ihrer Einheit die der Gruppe H. —

Wir wollen allgemeiner annehmen, dass die zu h gehörige Gruppe H nicht selbst autojug in G sei, aber eine Gruppe K als höchsten zu G autojugen Theiler enthalte. Bezeichnen wir mit τ die Substitutionen von K, so wird, weil $s^{-1}Ks = K$ ist, τ jeder Gruppe der zu (2) gehörigen Elemente angehören und also die Reihe (2) auch in ihrer Folge nicht ändern. Ist q_1 die Ordnung von K, so wird G zu H_0 in q_1-stufigem Isomorphismus stehen.

§ 579. Es ist naheliegend, nicht nur eine sondern alle Wurzeln $h_1, h_2, \cdots h_\varrho$ einer Resolventengleichung als bekannt anzusehen und sie sämmtlich zu adjungiren. Das bedeutet also, dass man die Resolventengleichung als vollständig aufgelöst annimmt.

Eine solche Adjunction ist nach unseren Ueberlegungen identisch mit derjenigen einer einzigen Function

$$(4)\quad k(z_1, z_2, \cdots z_n) = v_1 h_1(z_1, \cdots z_n) + v_2 h_2(z_1, \cdots z_n) + \cdots + v_\varrho h_\varrho(z_1, \cdots z_n),$$

in welcher $v_1, v_2, \cdots v_\varrho$ Unbestimmte bedeuten. Dadurch geht dann die Galois'sche Gruppe G in denjenigen Theiler K über, welcher alle gemeinsamen Substitutionen von

$$H,\ \sigma_2^{-1} H \sigma_2,\ \sigma_3^{-1} H \sigma_3,\ \cdots\ \sigma_\varrho^{-1} H \sigma_\varrho$$

enthält. Hieraus ersieht man, dass K sich unter dem Einflusse der Transformationen durch G nicht ändert; es wird, wenn s generell die Substitutionen von G bedeutet, daher

$$s^{-1} K s = K,$$

d. h. K ist der grösste autojuge Theiler von G, welcher in H enthalten ist. Adjungirt man der Gleichung $f(z) = 0$ von der Gattung G sämmtliche Wurzeln einer Resolventengleichung

(1), so reducirt sich dadurch die Gruppe G auf den höchsten autojugen Theiler K von G, welcher in der Gruppe H der Resolvente enthalten ist.

Ist daher die Gruppe einer Gleichung einfach (§ 552), so reducirt sie die Adjunction aller Wurzeln irgend einer Resolventengleichung (1) auf die Einheit; denn dies ist der einzige autojuge Theiler einer einfachen Gruppe. Nach § 552 findet dies bei jeder allgemeinen Gleichung statt, und auch wenn man solcher eine alternirende Function adjungirt.

Gehört dann aber $k(z_1, \cdots z_n)$ zur Gruppe 1, also zur Galois'schen Gattung, so ist jede rationale Function der Wurzeln und insbesondere die Galois'sche Resolvente ω_1 durch k rational darstellbar.

Sucht man durch derartige Adjunctionen der sämmtlichen Wurzeln von Resolventengleichungen die vorgelegte Gleichung $f(z) = 0$ zu lösen, dann braucht zwar nicht bei jeder Adjunction $f(z)$ selbst zu zerfallen; hingegen wird $\gamma(\omega)$ mehr und mehr zerlegt, weil ja der Grad jedes ihrer irreductiblen Factoren mit der Ordnung der Gruppe übereinstimmt, welche jedesmal die bekannte, adjungirte Gattung charakterisirt. Aber damit man zur definitiven Lösung von $f = 0$, d. h. zu seiner Zerfällung in lineare Factoren kommt, muss mindestens einmal bei solcher Adjunction auch f in rationale Factoren sich spalten. Es fragt sich, auf welche Weise dies geschehen kann.

Wir wollen annehmen, $f(z) = 0$ mit der Gruppe G sei noch irreductibel; durch die Adjunction aller Wurzeln η_α von (1) werde es reductibel, und G werde zugleich auf K reducirt. Dabei möge

$$(5) \qquad (z - z_1)(z - z_2) \cdots (z - z_\varkappa)$$

ein irreductibler, rationaler Factor von $f(z)$ werden. Die autojuge Gruppe K von G darf ihn nicht ändern; K kann also nur die Elemente $z_1, z_2, \cdots z_\varkappa$ unter einander transitiv verbinden. Nun ist aber G in $z_1, z_2, \cdots z_n$ transitiv und besitzt daher auch eine Substitution σ_2, welche die Folge $z_1 z_{\varkappa+1}$ enthält. Transformirt man K durch σ_2, so gehen $z_1, z_2, \cdots z_\varkappa$ in neue Elemente $z_{\varkappa+1}, \cdots$ über, die sämmtlich von den ersten verschieden sind, weil sonst $K = \sigma_2^{-1} K \sigma_2$ die früheren auch mit $z_{\varkappa+1}$ in Verbindung setzen würde. Es giebt also eine zweite Serie $z_{\varkappa+1}, \cdots z_{2\varkappa}$, die, wie leicht zu sehen ist, unter einander durch K transitiv verbunden sind, weil $z_1, \cdots z_\varkappa$ transitiv verbunden waren. Jede Substitution von G, welche auf ein Element der ersten Serie ein anderes derselben Serie folgen lässt, vertauscht nur diese $z_1, \cdots z_\varkappa$ unter einander; denn hätte man z. B. ein

$$\sigma = \begin{pmatrix} z_1 \cdots z_3 & \cdots \\ z_2 \cdots z_{k+1} & \cdots \end{pmatrix},$$

so würde aus $\sigma^{-1}K\sigma = K$ folgen, dass K auch z_2 mit z_{k+1} verbindet. Ebenso erkennt man, dass wenn eine Substitution von G auf ein Element der ersten Serie ein solches der zweiten folgen lässt, das Gleiche mit allen Elementen der ersten Serie stattfindet.

Giebt es noch andere Elemente ausser $z_1, \cdots z_\varkappa;\ z_{\varkappa+1}, \cdots z_{2\varkappa}$, so wiederholen sich die eben durchgeführten Schlüsse. Man erkennt auf diesem Wege: Die Elemente $z_1, z_2, \cdots z_n$ von G theilen sich in Systeme der Imprimitivität von je $\varkappa$ Wurzeln. G ist eine imprimitive Gruppe.

Falls umgekehrt G eine imprimitive Gruppe ist, und

$$z_{11}, \cdots z_{1m};\ z_{21}, \cdots z_{2m};\ \cdots\ z_{\mu 1}, \cdots z_{\mu m} \qquad (\mu m = n)$$

ihre in Systeme der Imprimitivität eingetheilten Wurzeln sind; falls ferner H derjenige (von der Einheit verschiedene) Theiler von G ist, welcher die Wurzeln jedes einzelnen Systems unter sich, nicht aber die Systeme unter einander vertauscht, dann erkennt man sofort, dass der Uebergang von G zu H ein Zerfallen von $f(z)$ in einzelne Factoren gleichen Grades m im Gefolge haben wird, so dass je die Wurzeln eines Systems diejenigen je eines rational darstellbaren Factors ausmachen. Dass H autojug in G ist, haben wir im § 575 gezeigt.

Ist G imprimitiv, dann findet durch den Uebergang zu H eine Zerfällung von $f(z)$ in nichtlineare Factoren statt. Ist G primitiv, dann ist nur durch den Uebergang zu dem Theiler 1 eine Zerfällung möglich; die einzelnen Factoren werden dabei linear.

Wir bemerken noch, dass auch bei Adjungirung einer einzigen Wurzel einer Resolventengleichung $f(z)$ zerfallen kann, dass dann aber die Factoren nicht nothwendiger Weise von demselben Grade sind. Man sieht dies an dem banalen Beispiele, in welchem man der Gleichung $f = 0$ die Resolvente z_1 selbst adjungirt; dann zerfällt nämlich $f(z)$ in einen Factor ersten und einen solchen $(n-1)^{\text{ten}}$ Grades.

Sechzigste Vorlesung.

Algebraische Zahlen.

§ 580. Wir haben uns früher bereits mit dem Begriffe des Rationalitätsbereiches vertraut gemacht (§ 47, Bd. I; § 314, Bd. I u. s. w.). Es ist der Bereich aller derjenigen rationalen Functionen und

Grössen, welche als rational bekannt anzusehen sind*). Bei der Fixirung eines solchen Bereiches genügt es, diejenigen Grössen anzugeben, aus denen sich alle seine als rational geltenden Grössen in Form rationaler Functionen mit ganzzahligen Coefficienten ableiten lassen. Sind solche darstellenden Grössen oder Elemente $\mathfrak{R}', \mathfrak{R}'', \cdots$ auf irgend eine Weise gewählt, dann mag die Klammer $(\mathfrak{R}', \mathfrak{R}'', \cdots)$ den Rationalitätsbereich andeuten. Die Wahl der Grössen $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \cdots$, d. h. also der Elemente eines Rationalitätsbereiches unterliegt an sich keinerlei Beschränkung, doch ist es für die Behandlung der algebraischen Fragen vollkommen bedeutungslos, transcendente Zahlengrössen oder transcendente Functionen von Variablen unter die Elemente mit aufzunehmen; denn die Resultate bleiben ungeändert, wenn an Stelle solcher transcendenten neue unabhängige Veränderliche gesetzt werden. Sind nämlich die Resultate der Theorie algebraischer Functionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \cdots$ erst für diesen Fall, wo die transcendenten $\mathfrak{R}$ durch unabhängige Variable ersetzt sind, entwickelt, so können dieselben, ihrer Natur und Herleitung nach, nur durch solche Specialisirung von Grössen $\mathfrak{R}$ alterirt oder modificirt werden, bei welcher algebraische Beziehungen zwischen denselben eintreten. Es kann daher unbeschadet der Allgemeinheit angenommen werden, dass die Elemente eines Rationalitätsbereiches aus einer Anzahl veränderlicher oder unbestimmter Grössen und algebraischer Functionen derselben bestehen, wobei unter einer algebraischen Function jede Wurzel einer Gleichung zu verstehen ist, deren Coefficienten rational bekannt sind. In dieser Vorlesung wollen wir uns der Betrachtung solcher Grössen zuwenden.

Die Wahl der $\mathfrak{R}$ ist, wie eben erwähnt wurde, keiner Beschränkung unterworfen. Bei gewissen Rationalitätsbereichen sind nun aber die constituirenden Elemente $\mathfrak{R}$ derartige, dass man den Bereich als einen natürlich abgegrenzten Bereich bezeichnen kann. Das findet zunächst statt für $(\mathfrak{R}') = (1)$, d. h. für den Bereich der gewöhnlichen rationalen Zahlen, welcher als der absolute, einfachste, in allen Rationalitätsbereichen enthalten ist, da ein jeder die Grösse $\mathfrak{R}' : \mathfrak{R}'$ ein-

---

*) Abel hat zuerst die Nothwendigkeit der Einführung dieses Begriffes erkannt: „Sur la résolution algébrique des équations", Oeuvres, publ. p. Lie et Sylow 2, p. 217; er glaubte aber den Fall transcendenter Grössen noch berücksichtigen zu müssen. Kronecker hat diese Begriffe weiter ausgestaltet (Berl. Ber., Juni 1853; Februar 1873; März 1879; Journ. f. Math. 92 [1882], p. 3 ff., p. 7 ff.). Vgl. auch Molk, Acta math. 6. — Dedekind gebraucht statt „Rationalitätsbereich" den Ausdruck „Körper", als „Vereinigung von zusammengehörigen Dingen, denen eine gewisse Vollständigkeit zukommt" (Weber, Algebra (2. Aufl.), I, § 146).

schliesst; dieser Bereich repräsentirt gewissermassen die absolute Einheit des Rationalitätsbegriffes. Ebenso sprechen wir auch in dem Falle von einem natürlichen Rationalitätsbereiche, wenn die $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \cdots$ sämmtlich unabhängige Variable bedeuten, und also $(\mathfrak{R}', \mathfrak{R}'', \cdots)$ alle rationalen Functionen derselben repräsentirt. In allen anderen Fällen haben wir es mit algebraisch abgegrenzten Bereichen zu thun; für sie hat Kronecker den Namen Gattungsbereich eingeführt.

§ 581. Ist $f(z)=0$ eine irreductible Gleichung n^{ten} Grades, deren Coefficienten einem gewissen Rationalitätsbereiche $(\mathfrak{R})$ angehören, und bezeichnen wir mit $z_1, z_2, \cdots z_n$ die Wurzeln von $f=0$, dann heisst jede derselben (vgl. den vorigen Paragraphen) eine algebraische Zahl oder Grösse n^{ter} Ordnung dieses Rationalitätsbereiches $(\mathfrak{R})$; die einzelnen $z_1, z_2, \cdots$ heissen zu einander conjuge Grössen in Hinsicht auf die Gleichung $f(z)=0$.

Wir wollen eine solche algebraische Zahl z_1, welche Wurzel der irreductiblen Gleichung $f(z)=0$ sein soll, dem Rationalitätsbereiche $(\mathfrak{R})$ adjungiren und ihn also zu $(\mathfrak{R}, z_1)$ erweitern; dann besteht dieser neue jetzt aus allen ganzen und gebrochenen rationalen Functionen $\frac{\varphi(z_1)}{\psi(z_1)}$, bei denen $\psi(z_1) \neq 0$ ist, und in denen sämmtliche Coefficienten von Zähler wie von Nenner dem Bereiche $(\mathfrak{R})$ angehören.

Diese allgemeine Form lässt sich vereinfachen. Da $\psi(z_1) \neq 0$ ist, so sind $\psi(z)$ und $f(z)$ theilerfremd, und es giebt ganze Functionen $\chi(z)$, $\varrho(z)$, für welche die Gleichung stattfindet

$$\chi(z) f(z) + \varrho(z)\psi(z) = 1.$$

Daraus folgt $\varrho(z_1) = 1 : \psi(z_1)$, d. h.

$$\frac{\varphi(z_1)}{\psi(z_1)} = \varphi(z_1)\varrho(z_1).$$

Man kann sich daher zunächst auf alle ganzen Functionen von z_1 beschränken, deren Coefficienten zu $(\mathfrak{R})$ gehören.

Setzt man weiter, indem die Division durch $f(z)$ ausgeführt wird, so lange es angeht,

$$\varphi(z)\varrho(z) = Q(z) f(z) + R(z) \qquad [R] < n,$$

dann ist für $z = z_1$, weil $f(z_1)$ verschwindet,

$$\frac{\varphi(z_1)}{\psi(z_1)} = R(z_1),$$

d. h. jede Grösse des Bereiches $(\mathfrak{R}, z_1)$ ist in der Form einer ganzen Function höchstens vom Grade $(n-1)$ darstellbar

$$R(z_1) = a_0 + a_1 z_1 + a_2 z_1^2 + \cdots + a_{n-1} z_1^{n-1},$$

deren Coefficienten dem Bereiche $(\mathfrak{R})$ angehören.

Die Grössen, welche aus $R(z_1)$ durch Eintragung der anderen Wurzeln entstehen

$$R(z_\alpha) = a_0 + a_1 z_\alpha + a_2 z_\alpha^2 + \cdots + a_{n-1} z_\alpha^{n-1} \qquad (\alpha = 1, 2, \cdots n),$$

heissen zu einander conjug. Ebenso heissen die Bereiche $(\mathfrak{R}, z_1)$, $(\mathfrak{R}, z_2), \cdots$ zu einander conjuge Bereiche.

Jede Grösse des Bereiches $(\mathfrak{R}, z_1)$ ist eine der oben gegebenen Definition entsprechende algebraische Zahl. Denn nehmen wir eine solche Grösse in der Form an

$$(1) \quad y_\alpha = a_0 + a_1 z_\alpha + a_2 z_\alpha^2 + \cdots + a_{n-1} z_\alpha^{n-1} \qquad (\alpha = 1, 2, \cdots n),$$

so wird das Product der n conjugen Werthe $(y - y_\alpha)$, nämlich

$$(2) \quad g(y) = (y - y_1)(y - y_2) \cdots (y - y_n) = y^n - b_1 y^{n-1} + \cdots \pm b_n$$

eine symmetrische Function der $z_1, z_2, \cdots z_n$, und die b werden demnach dem Rationalitätsbereiche $(\mathfrak{R})$ angehören. Jedes y_α ist somit Wurzel der Gleichung

$$(3) \qquad g(y) = 0$$

und also eine algebraische Zahl; denn sollte $g(y)$ reductibel sein, so kann man ja denjenigen passenden irreductiblen Factor $g_1(y)$ herausnehmen, dem y_α als Wurzelpunkt angehört.

Es ist von Interesse, zu wissen, ob und wann (3) zerfallen kann. $g_1(y)$ sei der irreductible Theiler von $g(y)$, welcher den Factor $(y - y_1)$ enthält. Die beiden Gleichungen in z

$$f(z) = 0 \quad \text{und} \quad g_1(a_0 + a_1 z + a_2 z^2 + \cdots + a_{n-1} z^{n-1}) = 0$$

haben die Wurzel $z = z_1$ gemeinsam und daher wegen der Irreductibilität der Function f alle Wurzeln von f. Folglich verschwindet $g_1(y)$ für alle conjugen Grössen (1). Sind alle conjugen Werthe (1) unter einander verschieden, dann ist (3) unzerlegbar, und y_1 eine algebraische Zahl n^{ter} d. h. derselben Ordnung wie z_1 selbst.

Sind hingegen die Werthe (1) nicht alle unter einander verschieden, dann wird $g_1(y)$ von geringerem Grade sein als $g(y)$. Ist hierbei $g_2(y)$ ein weiterer irreductibler Factor von $g(z)$, so wird ebenso geschlossen, dass die Gleichung in z

$$g_2(a_0 + a_1 z + a_2 z^2 + \cdots + a_{n-1} z^{n-1}) = 0$$

mit $f = 0$ eine und daher alle Wurzeln dieser Gleichung gemein hat. Deshalb muss dieses $g_2(a_0 + a_1 z + \cdots)$ mit jenem $g_1(a_0 + a_1 z + \cdots)$, d. h. $g_2(y)$

mit $g_1(y)$ zusammenfallen. Da Gleiches von allen einzelnen irreductiblen Factoren der Function $g(y)$ gilt, so folgt: Ist die Function (2) zerlegbar, so ist sie eine Potenz einer unzerlegbaren Function

$$(4) \qquad g(y) = g_1(y)^\nu.$$

In diesem Falle wird jedes y_α eine algebraische Zahl der Ordnung $\frac{n}{\nu} = q$.

§ 582. Es lassen sich in $(\mathfrak{R}, z_1)$ stets Zahlen y_1 bestimmen, welche von der n^{ten} Ordnung sind. Denn dazu ist es nach den bisherigen Resultaten ausreichend, die Coefficienten a so zu wählen, dass

$$\prod_{\alpha,\beta}\left(a_1(z_\alpha - z_\beta) + a_2(z_\alpha^2 - z_\beta^2) + \cdots + a_{n-1}(z_\alpha^{n-1} - z_\beta^{n-1})\right)$$
$$\binom{\alpha, \beta = 1, 2, \cdots n}{\alpha > \beta}$$

von Null verschieden bleibt; nach § 539 ist dies möglich. Uebrigens ist ja z_1 selbst von der n^{ten} Ordnung.

Ist y_1 eine derartige Zahl n^{ter} Ordnung, dann können wir umgekehrt auch z_1 durch y_1 und allgemein jedes z_α durch das entsprechende y_α darstellen. Denn der Ausdruck

$$g(y)\left[\frac{z_1}{y - y_1} + \frac{z_2}{y - y_2} + \cdots + \frac{z_n}{y - y_n}\right] = G(y)$$

ist eine ganze symmetrische Function der z_α, und also sind die einzelnen Glieder von G durch y und die Coefficienten von $f(z)$ darstellbar, d. h. sie gehören dem Bereiche $(\mathfrak{R}, y)$ an. Aus dieser Gleichung folgt für $y = y_1, y_2, \cdots$ wie gewöhnlich

$$(5) \qquad z_1 = \frac{G(y_1)}{g'(y_1)}, \quad z_2 = \frac{G(y_2)}{g'(y_2)}, \quad \cdots \quad z_n = \frac{G(y_n)}{g'(y_n)}.$$

Demnach kann man die beiden Bereiche einander gleich setzen:

$$(6) \qquad (\mathfrak{R}, z_\alpha) = (\mathfrak{R}, y_\alpha),$$

d. h. alle Grössen des einen so bestimmten Rationalitätsbereiches kommen gleichfalls in dem anderen Bereiche vor.

§ 583. Es fragt sich nun weiter, wann der eben behandelte Fall eintreten kann, dass nämlich $g(y)$ reductibel und also gleich einer Potenz, d. h. dass

$$(4) \qquad g(y) = g_1(y)^\nu \qquad (n = \nu \cdot q)$$

wird.

Es werde die irreductible Function g_1 in Linearfactoren zerlegt,

(7) $$g_1(y) = (y - y_1)(y - y_{\nu+1}) \cdots (y - y_{(\varrho-1)\nu+1}).$$

Wir wollen ferner annehmen, dass die ν Wurzeln von $g = 0$, welche gleich y_1 sind, durch

(8) $$y_1 = y_2 = y_3 = \cdots = y_\nu$$

gegeben werden, so dass demgemäss

(9) $$R(z_1) = R(z_2) = R(z_3) = \cdots = R(z_\nu)$$

ist, dass aber kein anderes y_α dem betrachteten Werthe y_1 gleich werde. Wendet man nun auf die Relationen (9) die Substitutionen der Gruppe G von $f(z) = 0$ an, so entstehen daraus gleichfalls gültige Relationen (§ 560; Schlusstheorem). Wenn daher eine Substitution von G den Werth y_1 in y_α $(\alpha \leq \nu)$ dadurch umwandelt, dass sie die Folge $z_1 z_\alpha$ besitzt, so werden durch sie die Werthe $y_1, y_2, \cdots y_\nu$ lediglich unter einander vertauscht, und deshalb ebenso die Werthe z_1, $z_2, \cdots z_\nu$, weil sonst noch andere Werthe in die Reihe (8) eintreten.

Da $f(z)$ irreductibel ist, so wird es weiter auch Substitutionen in der transitiven Gruppe G geben, welche z_1 in $z_{\nu+1}$ und also y_1 in $y_{\nu+1}$ umwandeln. Dadurch müssen dann alle Werthe (8) oder (9) in neue übergehen; und wir finden so die weiteren Relationen unter den y, welche aus (8), (9) stammen,

(8ᵃ) $$y_{\nu+1} = y_{\nu+2} = y_{\nu+3} = \cdots = y_{2\nu};$$

(9ᵃ) $$R(z_{\nu+1}) = R(z_{\nu+2}) = R(z_{\nu+3}) = \cdots = R(z_{2\nu}).$$

Die Substitutionen von G, welche auf eins der Glieder (8ᵃ) ein anderes folgen lassen, vertauschen diese Glieder sämmtlich nur unter sich. Geht man so fort, dann zeigt es sich, dass die Gruppe G von $f(z) = 0$ imprimitiv, und dass $f(z) = 0$ also selbst eine imprimitive Gleichung ist (§ 573).

Dasselbe Resultat kann man auch auf rein algebraischem Wege herleiten. Gelten die Formeln (4), (7), (8), (9), dann wird für jedes $\varkappa$ der Ausdruck

$$g_1(y)\sum_{\alpha=1}^{n}\frac{z_\alpha^\varkappa}{y - y_\alpha} = g_1(y)\left(\frac{z_1^\varkappa + \cdots + z_\nu^\varkappa}{y - y_1} + \frac{z_{\nu+1}^\varkappa + \cdots + z_{2\nu}^\varkappa}{y - y_{\nu+1}} + \cdots\right)$$

eine ganze symmetrische Function der Wurzeln z_α und kann daher gleich $G_1(y)$ gesetzt werden, wobei die Coefficienten von G_1 dem Bereiche $(\mathfrak{R})$ angehören. Nimmt man dann hierin an $y = y_1$, $y = y_{\nu+1}, \cdots$, so entstehen die Gleichungen

$$
(10)\qquad
\begin{aligned}
&z_1^\varkappa \;+ z_2^\varkappa \;+ \cdots + z_\nu^\varkappa = \frac{G_1(y_1)}{g_1'(y_1)}\,,\\
&z_{\nu+1}^\varkappa + z_{\nu+2}^\varkappa + \cdots + z_{2\nu}^\varkappa = \frac{G_1(y_{\nu+1})}{g_1'(y_{\nu+1})}\,, \qquad (\varkappa = 1, 2, \cdots \nu)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}
$$

Es kann demnach, wenn man die Newton'schen Formeln über den Zusammenhang der Wurzelpotenzen und der elementaren symmetrischen Functionen anwendet, hierdurch eine Gleichung

$$h(z;\,y) \equiv z^\nu - d_1(y)\,z^{\nu-1} + d_2(y)\,z^{\nu-2} - \cdots = 0$$

von der Beschaffenheit gefunden werden, dass $h(z;\,y_1) = 0$ die Wurzeln $z_1, z_2, \cdots z_\nu$ hat, $h(z;\,y_{\nu+1}) = 0$ die Wurzeln $z_{\nu+1}, \cdots z_{2\nu}$ u. s. w. Eliminirt man mithin aus den beiden Gleichungen

$$(11)\qquad g_1(y) = 0 \quad \text{und} \quad h(z;\,y) = 0$$

die Unbekannte y nach der Poisson'schen Methode, so findet sich

$$(12)\qquad f(z) = h(z;\,y_1)\cdot h(z;\,y_{\nu+1}) \cdots h(z;\,y_{(q-1)\nu+1}).$$

Folglich ist nach § 573 die Gleichung $f(z) = 0$ eine imprimitive Gleichung.

Wenn umgekehrt $f(z)$ eine Function von der Form (12), und also $f(z) = 0$ eine imprimitive Gleichung ist, dann giebt es Functionen

$$R(z_\alpha) = a_0 + a_1 z_\alpha + a_2 z_\alpha^2 + \cdots + a_{n-1} z_\alpha^{n-1},$$

welche mehr als einen, aber weniger als n von einander verschiedene Werthe besitzen. Zunächst ist ersichtlich, dass die symmetrischen Functionen von $z_1, z_2, \cdots z_\nu$ nur $n:\nu = q$ Werthe haben, und dass eine jede solche Function rational in y_1 ist $= \varphi(y_1)$, wie (10) zeigt. Weiter lässt sich nun y_1 durch z_1 allein rational darstellen. Denn aus (12) ist ersichtlich, dass $h(z_1;\,y_1) = 0$ ist, während $h(z_1;\,y) \neq 0$ wird für $y_{\nu+1}, y_{2\nu+1}, \cdots$. Folglich haben die beiden Gleichungen in y

$$(11^a)\qquad g_1(y) = 0 \quad \text{und} \quad h(z_1;\,y) = 0$$

nur die eine Wurzel $y = y_1$ gemeinsam, und der grösste gemeinsame Theiler beider Polynome in (11^a) wird $(y - y_1)$. Dieser lässt sich daher nach dem Euklid'schen Schema rational im Bereiche $(\mathfrak{R}, z_1)$ ausfindig machen, d. h. y_1 ist durch z_1 allein darstellbar

$$y_1 = a_0 + a_1 z_1 + a_2 z_1^2 + \cdots + a_{n-1} z_1^{n-1}.$$

Setzt man dies in $\varphi(y_1)$ ein, dann ist eine Function von z_1 mit mehr als einem und weniger als n Werthen gefunden.

Eine Grösse, welche von höherer Ordnung als der ersten, aber von geringerer als der n^{ten} ist, nennen wir eine imprimitive Grösse, solche Grössen dagegen, die von der n^{ten} Ordnung sind, primitive Grössen.

Durch eine primitive Grösse lässt sich jede andere (primitive oder imprimitive) des Rationalitätsbereiches $(\mathfrak{R}, z_1)$ rational darstellen. Die Darstellung einer primitiven Grösse durch eine imprimitive ist nicht möglich, wie schon die Verschiedenheit der Anzahlen ihrer Werthe zeigt.

Die bisherigen Resultate können wir folgendermassen zusammenfassen:

Nur wenn $f(z) = 0$ eine imprimitive Gleichung, also die Gruppe G von $f(z) = 0$ eine imprimitive Gruppe ist, giebt es im Rationalitätsbereiche $(\mathfrak{R}, z_\alpha)$ imprimitive Zahlen y_α. — Ist in $(\mathfrak{R}, z_\alpha)$ jede Grösse mit Ausnahme der zu $(\mathfrak{R})$ selbst gehörigen, welche ja von der Ordnung 1 sind, eine primitive, dann ist $f = 0$ eine primitive Gleichung. Jede irreductible Gleichung eines Primzahlgrades ist primitiv.

Einen Rationalitätsbereich $(\mathfrak{R}, z_1)$, welcher ausser den Grössen in $(\mathfrak{R})$ keine anderen imprimitiven enthält, nennen wir einen primitiven, jeden anderen einen imprimitiven Rationalitätsbereich.

§ 584. Für die weiteren Entwickelungen müssen wir die folgende Zwischenbetrachtung anstellen.

Es sei $g(t) = 0$ mit den Wurzeln $t_1, t_2, \cdots t_n$ eine beliebige irreductible Gleichung n^{ten} Grades, deren Coefficienten dem Rationalitätsbereiche $(\mathfrak{R})$ angehören. Ferner sei $h(u, t_1)$ eine in $(\mathfrak{R}, t_1)$ rationale Function von u und t_1 mit Coefficienten, die zu $(\mathfrak{R})$ gehören.

Wir nennen das Product

$$(13) \qquad N(h(u, t_1)) = h(u, t_1) \cdot h(u, t_2) \cdots h(u, t_n)$$

die Norm von $h(u, t_1)$ im Bereiche $(\mathfrak{R})$.

Die Norm eines Productes ist gleich dem Producte der Normen seiner Factoren, d. h.

$$N(h \cdot k) = N(h) \cdot N(k).$$

Wir wollen nun beweisen: Die Norm einer irreductiblen Function $h(u, t_1)$ ist entweder selbst irreductibel, oder sie ist eine Potenz einer in $(\mathfrak{R})$ irreductiblen Function. Dieser Satz umfasst den in § 581 bewiesenen als besonderen Fall in sich.

Wir denken uns die Norm (13) innerhalb $(\mathfrak{R})$ in irreductible Factoren zerlegt,

$$N(h(u, t_1)) = k_1(u) \cdot k_2(u) \cdots;$$

dann hat innerhalb $(\mathfrak{R}, t_1)$ der Factor $k_1(u)$ mit einem der Factoren aus (13), etwa mit $h(u, t_1)$, eine Nullstelle $u = \varpi$ gemeinsam. Man kann also setzen

$$k_1(\varpi) = 0, \quad h(\varpi, t_1) = 0.$$

In $(\mathfrak{R}, t_1)$ ist $h(u, t_1)$ irreductibel, deshalb ist $k_1(u)$ durch $h(u, t_1)$ theilbar, und wir können mithin $k_1(u)$ in die Form

$$k_1(u) = h(u, t_1) \cdot Q(u, t_1) \tag{14}$$

bringen, d. h. es haben die Gleichungen mit der Unbekannten t

$$k_1(u) - h(u, t) \cdot Q(u, t) = 0 \quad \text{und} \quad g(t) = 0$$

die Wurzel $t = t_1$ gemeinsam. Da $g(t)$ irreductibel ist, so hat die erste dieser beiden Gleichungen mit der zweiten alle Wurzeln gemeinsam, d. h. es gilt für jedes t_α die Gleichung

$$k_1(u) = h(u, t_\alpha) \cdot Q(u, t_\alpha) \qquad (\alpha = 1, 2, \cdots n). \tag{14a}$$

Statt dieses algebraischen Schlusses hätte man auch den Satz über die Galois'sche Gruppe benutzen können, um (14a) aus (14) abzuleiten; denn da $g(t)$ irreductibel ist, so muss die zu $g = 0$ gehörige Gruppe transitiv sein, und die Verwendung einer passenden Substitution würde den Uebergang liefern.

Das Gleiche ergiebt sich für $k_2(u)$; folglich haben $k_1(u) = 0$ und $k_2(u) = 0$ eine Wurzel ω und daher einen in $(\mathfrak{R})$ rationalen Factor gemeinsam. Weil beide irreductibel sind, so stimmen sie deshalb überein, und man hat also, wie behauptet wurde,

$$N(h(u, t_1)) = g_0 \cdot [k(u)]^\nu, \tag{15}$$

wobei g_0 eine dem Bereiche $(\mathfrak{R})$ angehörige Grösse bedeutet.

Ist $\nu = 1$, dann sind alle Wurzeln der Gleichungen

$$h(u, t_1) = 0, \quad h(u, t_2) = 0, \quad \cdots \quad h(u, t_n) = 0$$

von einander verschieden, weil $k = 0$ als irreductible Gleichung keine mehrfachen Wurzeln besitzt. Bezeichnet also u_1 irgend eine Wurzel von $h(u, t_1) = 0$, so wird

$$h(u_1, t_1) = 0; \quad h(u_1, t_2) \neq 0, \quad \cdots \quad h(u_1, t_n) \neq 0,$$

und es haben sonach die beiden Gleichungen

$$h(u_1, t) = 0, \quad g(t) = 0$$

nur die eine Wurzel $t = t_1$ gemeinsam. Folglich lässt sich der gemeinsame Theiler beider Gleichungspolynome $(t - t_1)$ rational durch u_1 mit Coefficienten in $(\mathfrak{R})$ darstellen, d. h. es wird bei $\nu = 1$ für eine jede Wurzel u_1 von $h(u, t_1) = 0$ eine Beziehung bestehen

$$t_1 = \varphi(u_1); \tag{16}$$

hierin bedeutet φ eine rationale Function des Bereiches $(\mathfrak{R})$.

Umgekehrt wollen wir annehmen, ohne über ν eine Voraussetzung zu machen, es sei möglich, t_1 durch eine Wurzel u_1 von $h(u, t_1) = 0$ in der Form (16) rational auszudrücken. Dann hat, wenn $u_1, u_2, \cdots u_m$ die Wurzeln von $k(u) = 0$ sind, die Gleichung

$$(t - \varphi(u_1))\,(t - \varphi(u_2)) \cdots (t - \varphi(u_m)) = 0$$

mit $g(t) = 0$ eine und also sämmtliche Wurzeln von $g = 0$ gemeinsam, d. h. es ist etwa

$$t_1 = \varphi(u_1), \quad t_2 = \varphi(u_2), \quad \cdots \quad t_n = \varphi(u_n),$$

und da $t_1, t_2, \cdots t_n$ von einander verschieden sind, so ist $m \geqq n$. Ferner hat die Gleichung

$$(t_1 - \varphi(u))\,(t_2 - \varphi(u)) \cdots (t_n - \varphi(u)) = 0$$

mit $k(u) = 0$ eine und also sämmtliche Wurzeln gemeinsam, d. h. es ist umgekehrt für $\alpha = 1, 2, \cdots m$ jedes $\varphi(u_\alpha)$ gleich einem t_β.

Sobald nun $m > n$ ist, müssen mehrere $\varphi(u_\alpha)$ einander gleich werden. Es seien alle Werthe der Reihe

$$\varphi(u_1) = \varphi(u_a) = \varphi(u_b) = \cdots = \varphi(u_d)$$

und nur sie einander gleich. Wendet man auf diese Relationen die Substitutionen der transitiven Gruppe G von $k(u) = 0$ an, so folgt, dass jede Substitution, die eins der $u_1, u_a, u_b, \cdots u_d$ auf ein anderes derselben Reihe folgen lässt, nur sie unter einander vertauscht; und dass jede Substitution, die auf eins derselben ein neues folgen lässt, lauter neue Elemente u hervorruft. So erkennen wir, dass G imprimitiv ist (§ 574), und wir können die $\varphi(u_\alpha)$ in Reihen von gleich vielen Elementen anordnen, bei denen wir die oben benutzten Indices $a, b, \cdots d$ durch bequemere ersetzen:

$$\begin{array}{l} \varphi(u_1) = \varphi(u_{n+1}) = \varphi(u_{2n+1}) = \cdots = \varphi(u_{(k-1)n+1}) \\ \varphi(u_2) = \varphi(u_{n+2}) = \varphi(u_{2n+2}) = \cdots = \varphi(u_{(k-1)n+2}) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \varphi(u_n) = \varphi(u_{2n}) \quad = \varphi(u_{3n}) \quad = \cdots = \varphi(u_{kn}) \end{array} \qquad (kn = m).$$

Hier bilden die Argumente jeder Reihe ein System der Imprimitivität.

Hieraus folgt, dass wegen $h(u_1, \varphi(u_1)) = 0$ und

$$h(u, t_1) = h(u, \varphi(u_1)) = h(u, \varphi(u_{n+1})) = \cdots = h(u, \varphi(u_{(k-1)n+1}))$$

die Gleichung

$$(17) \qquad h(u, t_1) = 0$$

die Grössen $u_1, u_{n+1}, u_{2n+1}, \cdots u_{(k-1)n+1}$ zu Wurzeln hat. Das sind aber auch die einzigen Wurzeln von (17). Denn das Product, welches jedenfalls als Factor in $h(u, t_1)$ vorkommt,

$$(u - u_1)(u - u_{n+1})(u - u_{2n+1}) \cdots (u - u_{(k-1)n+1}),$$

bleibt für die Gruppe von (17) ungeändert. Diese besteht nämlich aus denjenigen Substitutionen von G, welche die $u_1, u_{n+1}, \cdots$ nur unter sich vertauschen und also t_1 nicht ändern. Das angegebene Product ist folglich rational bekannt. Da aber $h(u, t_1)$ irreductibel ist, so fällt es mit diesem Producte zusammen.

Demnach ist (17) vom Grade k in u, und die linke Seite von (15) wird vom Grade $n \cdot k = m$; die rechte dagegen ist vom Grade $m \cdot \nu$. Folglich wird $\nu = 1$, d. h. $N(h(u, t_1))$ ist irreductibel.

Es ist charakteristisch für die Irreductibilität der Norm von $h(u, t_1)$, dass t_1 durch eine Wurzel der Gleichung $h(u, t_1) = 0$ rational darstellbar ist*).

§ 585. Wir wollen nun untersuchen, was eintritt, wenn wir eine Reihe von Adjunctionen nach einander machen, von denen jede folgende in dem Bereiche stattfindet, der durch die früheren festgelegt ist.

Es sei $(\mathfrak{R})$ ein natürlicher Rationalitätsbereich, und in ihm

$$f_1(z) = (z - z_1)(z - z_2) \cdots (z - z_n) = 0$$

eine irreductible Gleichung. Wir adjungiren zunächst z_1 und gelangen zu dem neuen Bereiche $(\mathfrak{R}, z_1)$. In diesem bilden wir wiederum eine irreductible Gleichung

$$f_2(y) = (y - y_1)(y - y_2) \cdots (y - y_m) = 0,$$

deren Coefficienten aber nicht nothwendig z_1 enthalten. Wir adjungiren y_1 und gelangen zu dem Bereiche $(\mathfrak{R}, z_1, y_1)$. Auch in diesem bilden wir eine irreductible Gleichung

$$f_3(x) = (x - x_1)(x - x_2) \cdots (x - x_l),$$

deren Coefficienten also y_1 und z_1 enthalten können aber nicht zu enthalten brauchen.

*) A. Kneser, Math. Ann. 30 (1887), p. 179 ff.

Ebenso erweitern wir den erhaltenen Rationalitätsbereich durch Adjunction von x_1 und bilden eine neue in $(\mathfrak{R}, x_1, y_1, z_1)$ irreductible Gleichung

$$f_4(u) \equiv (u - u_1)(u - u_2) \cdots (u - u_k) = 0,$$

in deren Coefficienten möglicherweise x_1, y_1, z_1 eingehen.

So kann man fortschreiten; wir bleiben aber, da dies für die Erkenntniss der Verhältnisse völlig ausreicht, hier stehen und betrachten den Bereich

$$(18) \qquad (\mathfrak{R}, u_1, x_1, y_1, z_1).$$

Es ist nicht ausgeschlossen, dass z. B. f_2 mit f_1 identisch ist, so dass z_1 und y_1 conjuge Grössen bedeuten, da sie Wurzeln einer und derselben irreductiblen Gleichung sind.

Den durch (18) definirten Bereich können wir dadurch vereinfachend umgestalten, dass wir zeigen: y_1, x_1 und u_1 sind Wurzeln je einer schon in $(\mathfrak{R})$ irreductiblen Gleichungen.

Um anzudeuten, dass die Coefficienten von $f_4(u)$ Functionen von x_1 sind, schreiben wir $f_4(u; x_1)$ und bilden nach § 584 die Norm von f_4 im Bereiche $(\mathfrak{R})$

$$N(f_4(u; x_1)) = f_4(u; x_1) \cdot f_4(u; x_2) \cdots f_4(u; x_l) \\ = [g_3(u)]^\nu.$$

Dann ist u_1 eine Wurzel der irreductiblen Gleichung $g_3(u) = 0$, deren Coefficienten dem Bereiche $(\mathfrak{R}, y_1, z_1)$ angehören. Kam x_1 in den Coefficienten von f_4 nicht vor, dann wird $f_4 = g_3$. Schreiben wir ausführlicher $g_3(u; y_1)$, dann wird die Norm dieses Ausdrucks

$$N(g_3(u; y_1)) = g_3(u; y_1) \cdot g_3(u; y_2) \cdots g_3(u; y_m) \\ = [g_2(u)]^\mu$$

die Potenz einer in $(\mathfrak{R}, z_1)$ irreductiblen Function, und u_1 eine Wurzel der in demselben Bereiche irreductiblen Gleichung $g_2(u) = g_2(u; z_1) = 0$. Endlich ergiebt die weitere Normbildung

$$N(g_2(u; z_1)) = g_2(u; z_1) \cdot g_2(u; z_2) \cdots g_2(u; z_n) \\ = [g_1(u)]^\varkappa$$

das Resultat, dass u_1 Wurzel einer in $(\mathfrak{R})$ irreductiblen Gleichung

$$g_1(u) = 0$$

wird, deren Coefficienten rationale Grössen in $(\mathfrak{R})$ sind. Die entsprechenden Resultate gelten für x_1 und für y_1.

§ 586. Eine weitere Vereinfachung von (18) erlangen wir durch den Satz, dass die Adjunction mehrerer algebraischer Grössen durch diejenige einer einzigen ersetzt werden kann. Wir wollen dies für den vorliegenden Fall zeigen, in welchem z_1, y_1, x_1, u_1 Wurzeln irreductibler Gleichungen in $(\mathfrak{R})$ von den Graden n, m, l und k sein sollen. Wir benennen die $k \cdot l \cdot m \cdot n$ Grössen

$$p_1 z_\alpha + p_2 y_\beta + p_3 x_\gamma + p_4 u_\delta \qquad (\alpha = 1, 2, \cdots n;\ \beta = 1, 2, \cdots m; \cdots)$$

in beliebiger Ordnung genommen $\varpi_1, \varpi_2, \cdots \varpi_{klmn}$. Dabei sollen p_1, p_2, p_3, p_4 Constanten sein, die wir so wählen können und wollen, dass keine zwei der ϖ_α einander gleich werden. Hierzu reicht es aus, den p solche Werthe zu geben, welche keiner der nur in endlicher Anzahl vorhandenen Gleichungen

$$p_1(z_\alpha - z_a) + p_2(y_\beta - y_b) + p_3(x_\gamma - x_c) + p_4(u_\delta - u_d) = 0$$
$$(\alpha, a = 1, 2, \cdots n;\ \beta, b = 1, 2, \cdots m; \cdots)$$

genügen.

Dann gehören die Coefficienten der Gleichung

$$P(\omega) \equiv (\omega - \varpi_1)(\omega - \varpi_2) \cdots (\omega - \varpi_{klmn}) = 0 \tag{19}$$

als symmetrische Functionen der Wurzeln des Gleichungssystems $f_1 = 0$, $f_2 = 0$, $f_3 = 0$, $f_4 = 0$ dem Gebiete $(\mathfrak{R})$ an. $P(\omega) = 0$ hat keine gleichen Wurzeln; es ist also $P'(\varpi_\alpha)$ von Null verschieden.

Bildet man nun etwa bei Bevorzugung von z vor y, x und u den Ausdruck

$$P(\omega) \sum_{\alpha,\beta,\gamma,\delta} \frac{z_\alpha}{\omega - p_1 z_\alpha - p_2 y_\beta - p_3 x_\gamma - p_4 u_\delta} = Q(\omega),$$

dann ist $Q(\omega)$ eine ganze Function in ω und den Wurzeln der vier Gleichungen $f = 0$; zugleich ist Q symmetrisch in den Wurzeln derselben, so dass die Coefficienten von $Q(\omega)$ zu $(\mathfrak{R})$ gehören. So folgt hieraus die Darstellung

$$z_\alpha = \frac{Q(p_1 z_\alpha + p_2 y_\beta + \cdots)}{P'(p_1 z_\alpha + p_2 y_\beta + \cdots)} = \frac{Q(\varpi_\varrho)}{P'(\varpi_\varrho)},$$

d. h. z_α ist eine rationale Function von ϖ_ϱ, in welcher der Nenner nicht verschwinden kann. Setzt man $p_1 z_1 + p_2 y_1 + p_3 x_1 + p_4 u_1 = \varpi_1$, so folgt die Darstellung von z_1 durch ϖ_1. Ebenso ergeben sich aber auch y_1, x_1, u_1. Man kann deswegen setzen

$$z_1 = \frac{Q(\varpi_1)}{P'(\varpi_1)}, \quad y_1 = \frac{R(\varpi_1)}{P'(\varpi_1)}, \quad x_1 = \frac{S(\varpi_1)}{P'(\varpi_1)}, \quad u_1 = \frac{T(\varpi_1)}{P'(\varpi_1)},$$

und es reicht also aus, statt gleichzeitig z_1, y_1, x_1, u_1 allein die eine Wurzel ϖ_1 von $P(\omega) = 0$ zu adjungiren, d. h. es ist

$$(20)\qquad (\mathfrak{R}, z_1, y_1, x_1, u_1) = (\mathfrak{R}, \varpi_1).$$

Die in § 585 gemachte mehrfache Adjunction führt demnach auch nur auf algebraische Zahlen, wie sie in § 581 definirt worden sind, und hiernach könnte es scheinen, als ob die Betrachtung dieser allein ausreichte und unsere neue Einführung gänzlich überflüssig wäre. Dies ist jedoch nicht der Fall. Denn wenn z. B. eine Wurzel von (19) dem Bereiche $(\mathfrak{R})$ adjungirt ist, dann kann die Umwandlung, wie sie durch (20) gegeben wird, dadurch wichtig und wesentlich werden, dass die Gleichungen $f_1 = 0, \cdots f_4 = 0$ von besonders hervorragenden, einfachen Eigenschaften sind, so dass hierdurch die Erkenntniss der Constitution von $(\mathfrak{R}, \varpi_1)$ gefördert wird. In der nächsten Vorlesung haben wir den hauptsächlichsten derartigen Fall eingehend zu besprechen.

§ 587. Die Einführung von ϖ_1 an Stelle von z_1, y_1, x_1, u_1 lässt die Frage entstehen, von welchem Grade derjenige in $(\mathfrak{R})$ irreductible Theiler von (19) sein wird, dem ϖ_1 als Wurzel genügt.

Wir betrachten zunächst nur $f_1(z) = 0$ vom n^{ten} Grade mit der Wurzel z_1 und $f_2(y) = 0$ vom m^{ten} Grade mit der Wurzel y_1; beide Gleichungen seien in dem Bereiche $(\mathfrak{R})$, dem ihre Coefficienten angehören, irreductibel.

Es möge nach Adjunction von z_1, also in $(\mathfrak{R}, z_1)$ die Function $f_2(y)$ in irreductible Factoren $k_1, k_2, \cdots$ zerfallen; wir schreiben

$$(21)\qquad f_2(y) = k_1(y; z_1) \cdot k_2(y; z_1) \cdot k_3(y; z_1) \cdots,$$

und k_1 sei derjenige dieser Factoren, dem y_1 als Wurzelpunkt angehört. Wir setzen

$$k_1(y; z_1) = (y - y_1)(y - y_2) \cdots (y - y_r).$$

Dann gilt für die Grösse $\omega = y + pz_1$, bei welcher p einen Parameter bedeutet, wie die Substitution zeigt, die Gleichung

$$k_1(\omega - pz_1; z_1) = K(\omega; z_1) = (\omega - [pz_1 + y_1]) \cdots (\omega - [pz_1 + y_r]).$$

Weil ferner nach (21)

$$f_2(y) - k_1(y; z) \cdot k_2(y; z) \cdot k_3(y; z) \cdots = 0$$

mit der irreductiblen Gleichung $f_1(z) = 0$ eine Wurzel z_1 gemeinsam hat, so gilt auch die Reihe der Gleichungen

$$(21^a)\qquad f_2(y) = k_1(y; z_\alpha) k_2(y; z_\alpha) k_3(y; z_\alpha) \cdots \qquad (\alpha = 1, 2, \cdots n),$$

und daraus ergiebt sich, dass jede der Gleichungen

$$k_1(\omega - pz_\alpha;\ z_\alpha) = K(\omega;\ z_\alpha) = 0 \qquad (\alpha = 1, 2, \cdots n)$$

als Wurzeln ω gewisse Grössen $(pz_\alpha + y_\beta)$ hat, in denen die y_β zu den Wurzeln von $f_2(y) = 0$ gehören. Die r zu einer solchen Gleichung gehörigen Wurzeln sind unter einander verschieden, da ja $k_1(y;\ z_\alpha)$ genau wie $k_1(y;\ z_1)$ irreductibel ist; und die zu den verschiedenen Gleichungen

$$K(\omega;\ z_1) = 0, \quad K(\omega;\ z_2) = 0, \quad \cdots \quad K(\omega;\ z_n) = 0$$

gehörigen Wurzeln sind gleichfalls von einander verschieden, falls p so bestimmt ist, wie dies zu Beginn von § 586 geschah; denn die Coefficienten von p sind ja von einander verschieden.

Bildet man also die Norm von $k_1(\omega - pz_1;\ z_1)$, nämlich

$$N(k_1(\omega - pz_1;\ z_1)) = K(\omega;\ z_1) \cdot K(\omega;\ z_2) \cdots K(\omega;\ z_n),$$

dann ist dies eine in $(\mathfrak{R})$ rationale Function, welche als Potenz einer irreductiblen Function auftritt (§ 584). Nach dem soeben Bewiesenen hat aber diese Norm keine mehrfachen Wurzelwerthe; folglich ist sie selbst schon irreductibel.

Weil $k_1(y;\ z_\alpha)$ den Grad r besitzt, so steigt die Norm in ω bis zum Grade $n \cdot r$ auf; d. h.: Wenn nach Adjunction von z_1 die Gleichung m^{ten} Grades $f_2(y) = 0$ zerfällt, und der Factor $k_1(y;\ z_1)$, welcher gleich Null gesetzt y_1 zur Wurzel hat, vom Grade r ist, dann hängt $\overline{\omega}_1 = pz_1 + y_1$ von einer irreductiblen Gleichung des Grades nr ab, deren Coefficienten rational in $(\mathfrak{R})$ sind; dabei bedeutet p eine unbestimmte Grösse.

Vertauscht man in der Beweisführung f_1 und f_2, adjungirt man also zunächst y_1 und betrachtet die dann etwa erfolgende Zerfällung von f_1 in irreductible Factoren, wobei s der Grad des Factors sein mag, der gleich Null gesetzt z_1 als Wurzel giebt, dann zeigt sich ebenso, dass ω die Wurzel einer Gleichung des Grades ms ist. Hieraus ziehen wir den Schluss: Sind z_1 und y_1 Wurzeln bezw. von

$$f_1(z) = 0 \quad \text{und} \quad f_2(y) = 0,$$

zweier in $(\mathfrak{R})$ irreductiblen Gleichungen der Grade n bezw. m; ist ferner r der Grad derjenigen nach Adjunction von z_1 irreductiblen Gleichung, welcher y_1 genügt, und s der Grad derjenigen nach Adjunction von y_1 irreductiblen Gleichung, welcher z_1 genügt, so gilt die Proportion $n : m = s : r$.

Von dem ersten der beiden Resultate kann man nun zu dem Falle dreier Gleichungen $f_1(z) = 0$, $f_2(y) = 0$, $f_3(x) = 0$ fortschreiten, indem man die Adjunction von z_1 und y_1 zunächst durch diejenige einer Wurzel ϖ_1 von $N(K_1(\omega; z_1)) = 0$ ersetzt und darauf von ϖ_1 zu $(x_1 + p_1\varpi_1)$ übergeht. Man gelangt dadurch zu dem Resultate: Genügt z_1 im Bereiche $(\mathfrak{R})$ einer irreductiblen Gleichung vom Grade r_1; ferner y_1 im Bereiche $(\mathfrak{R}, z_1)$ einer irreductiblen Gleichung des Grades r_2; und endlich x_1 im Bereiche $(\mathfrak{R}, y_1, z_1)$ einer irreductiblen Gleichung des Grades r_3, so hängt die Grösse $\varpi_1 = x_1 + p_1 y_1 + p_2 z_1$, durch welche x_1, y_1, z_1 rational darstellbar sind, als Wurzel von einer irreductiblen Gleichung des Grades $r_1 \cdot r_2 \cdot r_3$ ab. Der allgemeine Satz ist hiernach klar. (Vgl. A. Kneser l. c.)

§ 588. Wir haben in den vorhergehenden Paragraphen dieser Vorlesung die Aufgabe als gelöst angesehen, eine Function innerhalb eines Gattungsbereiches in ihre irreductiblen Factoren zu zerlegen. Es ist jedoch zu bemerken, dass das Problem der Zerlegung bisher nur für natürliche Rationalitätsbereiche behandelt und erledigt worden ist (§ 50, Bd. I und § 341); an erster Stelle für den natürlichen Rationalitätsbereich $(\mathfrak{R}) = 1$, an letzterer für $(\mathfrak{R}, \mathfrak{R}', \cdots) = (1, z_2, z_3, \cdots)$, indem wir $f(z_1)$ mit Coefficienten dieses Bereiches versehen dachten, der aus lauter Unbestimmten $z_2, z_3, \cdots$ zusammengesetzt war.

Die allgemeinste Zerlegungsaufgabe würde sich auf eine Function $g(z_1, z_2, \cdots z_n)$ beziehen, deren Coefficienten in einem Gattungsbereiche $(\mathfrak{R}, \mathfrak{R}', \mathfrak{R}'', \cdots)$ enthalten sind; wie kann man g innerhalb dieses Rationalitätsbereiches in irreductible Factoren zerlegen?

Zunächst kann man die Frage so umgestalten, dass man eine Variable z allein als Argument von g ansieht und die übrigen in den Rationalitätsbereich verweist (§ 343, V); weiter kann man den Rationalitätsbereich so zubereiten, dass er ausser unbestimmten Grössen nur eine einzige algebraische Zahl enthält [§ 586; (20)].

Hiernach reicht es aus, die Zerlegung

$$(22) \qquad f(z; \varpi_1) = g_1(z; \varpi_1) \cdot g_2(z; \varpi_1) \cdot g_3(z; \varpi_1) \cdots$$

der Function f in irreductible Factoren g_α des Gebietes $(\varpi_1, \mathfrak{R}', \mathfrak{R}'', \cdots)$ zu fordern, wobei die $\mathfrak{R}', \mathfrak{R}'', \cdots$ Unbestimmte bedeuten, und ϖ_1 die Wurzel einer irreductiblen Gleichung

$$P(\omega) \equiv (\omega - \varpi_1)(\omega - \varpi_2) \cdots (\omega - \varpi_m) = 0$$

ist, deren Coefficienten dem Bereiche $(\mathfrak{R}', \mathfrak{R}'', \cdots)$ angehören. Endlich kann man ohne Beschränkung annehmen, dass $f(z; \varpi_1)$ von mehrfachen

Theilern frei sei, und dass auch kein gemeinsamer Factor aller Coefficienten von $f(z;\,\omega_1)$ besteht.

Wir wollen in (22) statt z eintragen $z = x + t\varpi_1$, wobei t ein unbestimmter Parameter sein soll. Das hat zwei Vorzüge im Gefolge. Zuerst tritt in den Coefficienten der Potenzen von x in f jetzt wirklich die Grösse ω_1 auf, was für uns von Gewicht ist, während das bisher nicht nöthig war; zweitens wird dabei die Norm von $f(x + t\omega_1)$ keine Potenzen als Factoren enthalten.

Gesetzt nämlich man hätte

$$N(f(x + t\omega_1;\,\omega_1)) = Q_1^{\varkappa_1}(x)\cdot Q_2^{\varkappa_2}(x)\cdot Q_3^{\varkappa_3}(x)\cdots$$

als Zerlegung der Norm im Gebiete $(\Re', \Re'', \cdots)$, dann würde, wenn auch nur einer der Exponenten $\varkappa$ grösser wäre als 1, $N(f)$ mit seiner Ableitung einen gemeinsamen Theiler haben, also

$$f(x + t\varpi_1;\,\varpi_1)\cdot f(x + t\varpi_2;\,\varpi_2)\cdots f(x + t\varpi_m;\,\varpi_m)$$

mit

$$f(x + t\varpi_1;\,\varpi_1)\cdots f(x + t\varpi_m;\,\varpi_m)\sum_{\alpha=1}^{m}\frac{f'(x + t\varpi_\alpha;\,\varpi_\alpha)}{f(x + t\varpi_\alpha;\,\varpi_\alpha)}.$$

Kommt derselbe nun etwa in $f(x + t\varpi_1;\,\varpi_1)$ vor, so müsste, weil $f(x + t\varpi_1;\,\varpi_1)$ von mehrfachen Factoren frei ist und also mit $f'(x + t\varpi_1;\,\varpi_1)$ keinen gemeinsamen Theiler hat, ein solcher etwa für die beiden Functionen

$$f(x + t\varpi_1;\,\varpi_1) \quad \text{und} \quad f(x + t\varpi_2;\,\varpi_2) \tag{23}$$

bestehen. Auf die Irreductibilität von $f(x + t\varpi_1;\,\varpi_1)$ können wir uns, um diese Eventualität abzuweisen, hier nicht berufen, weil Irreductibilität im Bereiche $(\varpi_1, \varpi_2, \Re', \Re'', \cdots)$ nicht zu gelten braucht. Aber auf anderem Wege lässt sich leicht die Unmöglichkeit der Existenz eines gemeinsamen Factors für (23) zeigen. Wir setzen $x + t\varpi_1 = y$, dann giebt die erste jener Functionen $f(y;\,\varpi_1)$ und die zweite

$$f(y + t(\varpi_2 - \varpi_1);\,\varpi_2)$$
$$= f(y;\,\varpi_2) + t(\varpi_2 - \varpi_1)\cdot f'(y;\,\varpi_2) + \cdots + t^q(\varpi_2 - \varpi_1)^q.$$

Wegen der Unbestimmtheit von t müssten $f(y;\,\varpi_1)$ und $(\varpi_2 - \varpi_1)^q$ einen gemeinsamen Theiler besitzen, d. h. $(\varpi_2 - \varpi_1)$ müsste Factor aller Coefficienten von f werden. Die Existenz eines solchen war aber ausgeschlossen. Es sind demnach alle $\varkappa$ gleich 1 zu setzen, und man hat*)

$$N(f(x + t\varpi_1;\,\varpi_1)) = Q_1(x)\cdot Q_2(x)\cdot Q_3(x)\cdots, \tag{24}$$

---

*) Molk, Acta math. 6, p. 41 ff. — Kronecker, Journ. f. Math. 91 (1882), p. 12. — Kneser l. c., p. 187.

wobei die Q von einander verschiedene rationale irreductible Functionen in $(\mathfrak{R}', \mathfrak{R}'', \cdots)$ bedeuten.

Wir suchen nun nach dem Euklid'schen Algorithmus den grössten gemeinsamen Theiler von $Q_1(x)$ und $f(x + t\varpi_1;\, \varpi_1)$, indem wir beide Functionen von x in bekannter Weise behandeln und $P(\varpi_1) \equiv 0$ zur Reduction der Coefficienten benutzen. Dieser Theiler sei $\varphi(x;\, \varpi_1)$, und es werde gesetzt

$$\varphi(x;\, \varpi_1) \cdot \varphi_1(x;\, \varpi_1) = Q_1(x),$$
$$\varphi(x;\, \varpi_1) \cdot \varphi_2(x;\, \varpi_1) = f(x + t\varpi_1;\, \varpi_1).$$

Das ergiebt dann, wenn man die Normen nimmt,

$$N(\varphi(x;\, \varpi_1)) \cdot N(\varphi_1(x;\, \varpi_1)) = Q_1^m(x),$$
$$N(\varphi(x;\, \varpi_1)) \cdot N(\varphi_2(x;\, \varpi_1)) = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdots.$$

Aus der ersten dieser Gleichungen schliesst man, dass $N(\varphi)$ eine Potenz von Q_1 wird und aus der zweiten, dass der Exponent dieser Potenz 1 ist; folglich wird zu setzen sein

$$N(\varphi(x;\, \varpi_1)) = Q_1.$$

Daraus folgt weiter, dass $\varphi(x;\, \varpi_1)$ irreductibel wird, denn nach § 560 würde sonst folgen, dass Q_1 auch zerlegbar wäre. Es ist demnach der grösste gemeinsame Theiler von $f(x + t\varpi_1;\, \varpi_1)$ und Q_1 einer der irreductiblen Factoren von $f(x + t\varpi_1;\, \varpi_1)$. Durch die grössten gemeinsamen Theiler von

$$f(x + t\varpi_1;\, \varpi_1) \quad \text{mit} \quad Q_1,\ Q_2,\ Q_3,\ \cdots$$

werden sämmtliche irreductiblen Factoren von f geliefert. Setzt man in ihnen dann $x = z - t\varpi_1$, so erhält man die Zerlegung von $f(z;\, \varpi_1)$ in seine irreductiblen Theiler innerhalb des Bereiches $(\varpi_1, \mathfrak{R}', \mathfrak{R}'', \cdots)$. Damit ist die gestellte Aufgabe gelöst, und die Irreductibilitätsuntersuchungen sind auch für Gattungsbereiche erledigt.

§ 589. Wir wollen eine praktische Anwendung für die Methode zeigen, eine Function innerhalb eines gegebenen Gattungsbereiches zu zerlegen, indem wir die Reductibilität oder Irreductibilität der Function

$$f(z) = \Theta_1(\Theta_2(z)) \tag{25}$$

untersuchen, in welcher Θ_1 und Θ_2 ganze Functionen sein sollen, deren Coefficienten dem Rationalitätsbereiche $(\mathfrak{R})$ angehören. Diese Untersuchungen stammen von A. Capelli*).

*) Rend. d. R. Acc. d. Napoli. (1897) Dicembre; (1898) Febbraio; Maggio.

Als erste Bedingung für die Irreductibilität von f innerhalb $(\mathfrak{R})$ erkennt man die Irreductibilität von $\Theta_1(y)$ innerhalb des gleichen Bereiches. Diese Bedingung sei erfüllt; dann sind die Wurzeln von

$$\Theta_1(y) = (y - y_1)(y - y_2) \cdots (y - y_m) = 0$$

von einander verschieden. Aus dieser Gleichung folgt

$$f(z) = \Theta_1(\Theta_2(z)) = (\Theta_2(z) - y_1)(\Theta_2(z) - y_2) \cdots (\Theta_2(z) - y_m).$$

Gesetzt der Factor $\Theta_2(z) - y_1$ wäre im Gebiete $(\mathfrak{R}; y_1)$ reductibel, was wir nach dem vorigen Paragraphen prüfen können, und es wäre

$$\Theta_2(z) - y_1 = \vartheta_1(z; y_1) \cdot \vartheta_0(z; y_1),$$

wobei ϑ_1, ϑ_0 rationale ganze Functionen von z und y_1 mit Coefficienten aus $(\mathfrak{R})$ sind, dann gilt

$$\Theta_2(z) - y_\varkappa = \vartheta_1(z; y_\varkappa) \cdot \vartheta_0(z; y_\varkappa) \qquad (\varkappa = 1, 2, \cdots m),$$

weil die vorhergehende Gleichung mit der irreductiblen Gleichung $\Theta_1(y) = 0$ eine Wurzel gemeinsam hat. Deswegen wird

$$\begin{aligned} f(z) &= \prod \vartheta_1(z; y_\varkappa) \cdot \prod \vartheta_0(z; y_\varkappa) \qquad (\varkappa = 1, 2, \cdots m) \\ &= T_1(z) \cdot T_0(z). \end{aligned}$$

Die T sind hier ganze Functionen in $(\mathfrak{R})$, und $f(z)$ ist daher reductibel.

Wir zeigen weiter, dass T_1 in $(\mathfrak{R})$ irreductibel ist, falls $\vartheta_1(z; y_1)$ es in $(\mathfrak{R}; y_1)$ ist. Hätte $T_1(z)$ den Factor $\tau(z)$, so müsste dieser mit einer der Functionen $\vartheta_1(z; y_\varkappa)$ einen Theiler gemeinsam haben, z. B. mit $\vartheta_1(z; y_1)$. Da $\vartheta_1(z; y_1)$ als irreductibel in $(\mathfrak{R}; y_1)$ vorausgesetzt wird, so muss demnach $\vartheta_1(z; y_1)$ die Function $\tau(z)$ theilen:

$$\tau(z) = \vartheta_1(z; y_1) \cdot \vartheta_0(z; y_1).$$

Ersetzt man hierin y_1 durch $y_2, \cdots y_m$, so sind auch die neu entstehenden Gleichungen richtig, weil $\Theta_1(y) = 0$ irreductibel ist. Folglich sind alle m Functionen

$$(26) \qquad \vartheta_1(z; y_1), \quad \vartheta_1(z; y_2), \quad \cdots \quad \vartheta_1(z; y_m)$$

Theiler von $\tau(z)$. Keins der ϑ_1 liefert, gleich Null gesetzt, mehrfache Wurzeln. Ferner haben aber auch nicht zwei Gleichungen

$$\vartheta_1(z; y_i) = 0, \quad \vartheta_1(z; y_k) = 0$$

gemeinsame Wurzeln. Denn wäre ζ eine solche, so hätte man

$$\begin{aligned} \Theta_2(\zeta) - y_i &= \vartheta_1(\zeta; y_i) \cdot \vartheta_0(\zeta; y_i) = 0, \\ \Theta_2(\zeta) - y_k &= \vartheta_1(\zeta; y_k) \cdot \vartheta_0(\zeta; y_k) = 0, \end{aligned}$$

d. h. es wäre gegen die Annahme der Irreductibilität von $\Theta_1(y)$ gleichwohl $y_i = y_k$.

Es enthält daher $\tau(z)$ das Product der Functionen (26), d. h. $\tau(z)$ fällt mit $T_1(z)$ zusammen.

Zerlegt man also im Rationalitätsbereiche $(\mathfrak{R}; y_1)$ die Differenz $(\Theta_2(z) - y_1)$ in ihre irreductiblen Factoren

$$\Theta_2(z) - y_1 = \vartheta_1(z; y_1) \cdot \vartheta_2(z; y_1) \cdots \vartheta_\nu(z; y_1),$$

dann sind

$$\prod_\varkappa \vartheta_1(z; y_\varkappa), \quad \prod_\varkappa \vartheta_2(z; y_\varkappa), \quad \cdots \quad \prod_\varkappa \vartheta_\nu(z; y_\varkappa) \qquad (\varkappa = 1, 2, \cdots m)$$

die in $(\mathfrak{R})$ irreductiblen Factoren von

$$\Theta_1(\Theta_2(z)). \tag{25}$$

Die Ordnung jedes dieser irreductiblen Factoren ist ein Vielfaches von m, d. h. vom Grade der Function $\Theta_1(y)$.

Für die Irreductibilität von (25) ist es charakteristisch, dass $\Theta_1(z)$ in $(\mathfrak{R})$ und $\Theta_2(z) - y_1$ in $(\mathfrak{R}; y_1)$ irreductibel sind.

Hieran schliesst sich folgendes Theorem. Es sei

$$f(z) = \Theta_1(\Theta_2(z)) = \chi_1(\chi_2(z)), \tag{25a}$$

wobei $\Theta_1(z)$ sowie $\chi_2(z)$ vom Grade m, und $\Theta_2(z)$ sowie $\chi_1(z)$ vom Grade n sind. Die Zahlen m und n seien theilerfremd. Dann ist es für die Irreductibilität von (25a) im Bereiche $(\mathfrak{R})$ charakteristisch, dass $\Theta_1(z)$ und $\chi_1(z)$ in demselben Bereiche irreductibel seien.

Dass diese Bedingungen nothwendig sind, ist klar. Sie sind aber auch hinreichend. Denn ist $\tau(z)$ ein irreductibler Theiler von $f(z)$, dann muss sein Grad nach dem vorigen Satze ein Vielfaches von m wie von n und also von mn sein; d. h. der Theiler fällt mit $f(z)$ zusammen.

§ 590. Diese beiden Theoreme benutzt Capelli, um die Irreductibilitätsfragen für die binomische Gleichung

$$z^n - A = 0 \tag{27}$$

in einem beliebigen Rationalitätsbereich $(\mathfrak{R})$, dem A angehört, zu entscheiden.

Es sei in seine verschiedenen Primzahlpotenzen zerlegt

$$n = p^\alpha q^\beta r^\gamma \cdots = p^\alpha \cdot \nu.$$

Wir setzen

$$\Theta_1(z) = z^{p^\alpha} - A, \quad \Theta_2(z) = z^\nu; \quad \chi_1(z) = z^\nu - A, \quad \chi_2(z) = z^{p^\alpha},$$

dann folgt, dass (27) dann und nur dann irreductibel ist, wenn es die beiden Gleichungen

$$z^{p^\alpha} - A = 0, \quad z^{\nu} - A = 0$$

sind. Wendet man auf die zweite dieselben Schlüsse an und geht so fort, dann kommt man zu dem Satze: Für die Irreductibilität von

$$z^n - A = 0, \quad n = p^\alpha q^\beta r^\gamma \cdots \tag{27}$$

ist es charakteristisch, dass

$$z^{p^\alpha} - A = 0, \quad z^{q^\beta} - A = 0, \quad z^{r^\gamma} - A = 0, \quad \cdots$$

innerhalb $(\mathfrak{R})$ irreductibel sind.

Hierdurch ist die Frage also auf binomische Gleichungen vom Primzahlpotenzgrade reducirt. Wir betrachten deswegen jetzt nur

$$z^{p^\alpha} - A = 0 \tag{28}$$

und setzen

$$\Theta_1(z) = z^p - A, \quad \Theta_2(z) = z^{p^{\alpha-1}}.$$

$\Theta_1(z) = z^p - A$ ist innerhalb $(\mathfrak{R})$ irreductibel, sobald in dem gleichen Bereiche A nicht eine vollständige p^{te} Potenz ist. Diesen Satz wollen wir als richtig voraussetzen; er wird in der folgenden Vorlesung, unabhängig von unseren jetzigen Betrachtungen, im § 594 bewiesen werden.

Wäre A keine solche vollständige p^{te} Potenz, dann könnte trotzdem (28) noch reductibel sein, wenn nämlich gemäss dem ersten Lehrsatze des vorigen Paragraphen

$$\Theta_2(z) - y_1 = z^{p^{\alpha-1}} - y_1 \tag{29}$$

es in $(\mathfrak{R}; y_1)$ ist. Dabei bedeutet y_1 eine Wurzel von

$$\Theta_1(y) = y^p - A = (y - y_1)(y - y_2)\cdots(y - y_p) = 0.$$

Es fragt sich also, ob (29) in $(\mathfrak{R}; y_1)$ reductibel oder irreductibel ist. Diese Gleichung ist der Gleichung (28) völlig ähnlich, da ja, wie wir nachweisen wollen, y_1 im Gebiete $(\mathfrak{R}; y_1)$ auch keine vollständige p^{te} Potenz ist. Wäre nämlich

$$y_1 = [h(y_1)]^p,$$

so würde die Gleichung, welche durch Eintragung von y_i statt y_1 entsteht, auch richtig sein, da $y^p - A = 0$ irreductibel ist. Folglich wäre

$$y_1 y_2 \cdots y_p = [h(y_1) \cdot h(y_2) \cdots h(y_p)]^p.$$

Ist nun p eine ungerade Primzahl, dann wird die linke Seite gleich A, während die eckige Klammer auf der rechten Seite dem Bereiche $(\mathfrak{R})$

angehört. Folglich wäre A gegen die Annahme eine vollständige p^{te} Potenz. Für $p = 2$ gilt dieser Schluss nicht, da für $p = 2$ die linke Seite zu $(-A)$ würde.

Wir setzen jetzt $p > 2$ voraus und haben dann in (29) das vollkommene Analogon von (28), sobald wir $(\mathfrak{R}; y_1) = (\mathfrak{R}')$ setzen. Dieselben Schlüsse gelten weiter, d. h. (29) ist nur dann reductibel, wenn die binomische Gleichung $(p^{\alpha-2})^{ten}$ Grades es ist, welche daraus hergeleitet werden kann, nämlich

$$z^{p^{\alpha-2}} - y_1' = 0,$$

u. s. f. So kommt man endlich auf eine Gleichung des Grades p

$$z^p - y_1^{(\alpha-2)} = 0,$$

worin $y_1^{(\alpha-2)}$ keine vollständige p^{te} Potenz im entsprechenden Rationalitätsbereiche wird. Folglich ist diese Gleichung irreductibel, und damit zugleich auch (28). Dafür dass

$$(28) \qquad z^{p^\alpha} - A = 0 \qquad (p > 2)$$

irreductibel in $(\mathfrak{R})$ sei, ist es charakteristisch, dass A in dem gleichen Rationalitätsbereiche keine vollkommene p^{te} Potenz wird.

Wie schon bemerkt wurde, gilt der Beweis nicht für den Fall $p = 2$. Aber auch der Satz selbst muss hierbei modificirt werden, wie das Beispiel

$$z^4 - A \equiv z^4 + 4b^4 = (z^2 - 2bz + 2b^2)(z^2 + 2bz + 2b^2)$$

zeigt, in welchem Zerlegung stattfindet, trotzdem A kein Quadrat ist. Es ist also für Potenzen von 2 ein Ergänzungssatz nöthig. Capelli leitet diesen in der zweiten der angeführten Noten ab. Wir begnügen uns, ohne den dort gegebenen Beweis zu reproduciren, mit der Angabe des Theorems: Dafür dass

$$z^{2^\lambda} - A = 0$$

in einem gegebenen Rationalitätsbereiche reductibel sei, ist es charakteristisch, dass entweder A in diesem Bereiche ein Quadrat, oder dass $-A$ in ihm das Vierfache einer vierten Potenz bildet.

§ 591. Wir haben in unseren Untersuchungen die Möglichkeit angenommen, dass durch Adjunction einer Wurzel y_1 von $f_2(y) = 0$ des Grades m die Gleichung $f_1(z) = 0$ des Grades n in Factoren zerfällt. Dass derartige Verhältnisse eintreten können, ist ersichtlich, wenn man $f_2 \equiv f_1$ setzt. Wir fragen nach den allgemeinen Bedingungen, unter denen ein solcher Fall von Zerlegung vorkommt.

Ist nach Adjunction von y_1 zu $f_1(z) = 0$ die Function

$$h_1(z) = (z - z_1)(z - z_2) \cdots (z - z_\nu) \qquad (\nu < n)$$

ein irreductibler Factor von $f_1(z)$, dann heisst dies, dass die symmetrischen Functionen von $z_1, z_2, \cdots z_\nu$ rational durch y_1 darstellbar sind.

Gesetzt $\varphi(z_1, \cdots z_n)$ und $\psi(z_1, \cdots z_n)$ wären beide durch y_1 darstellbar, dann ist es auch

$$\varphi(z_1, \cdots z_n) + u\psi(z_1, \cdots z_n).$$

Daraus folgt, dass es eine kleinste Gruppe K_1 giebt, derart, dass alle zu ihrer Gattung und unter ihr stehenden Functionen, aber keine andere rational durch y_1 ausdrückbar ist. Bezeichnen wir mit $k_1(z_1, \cdots z_n)$ jede zu K_1 gehörige Function, dann ist also

$$k_1(z_1, z_2, \cdots z_n) = R(y_1).$$

Andrerseits ist durch $R(y_1)$ eine Gattung der y bestimmt, zu der entweder y_1 gehört, oder über der y_1 steht. Ihre Gruppe mag K_2 sein; $k_2(y_1, \cdots y_m)$ bedeute jede zu K_2 gehörige Function. Dann ist durch k_1 jede zu K_2 gehörige und durch k_2 jede zu K_1 gehörige Function rational darstellbar. Dies bedeutet: Die Gattung K_1 der $z_1, z_2, \cdots z_n$ stimmt mit der Gattung K_2 der $y_1, y_2, \cdots y_m$ überein.

Wenn umgekehrt für f_1 und f_2 zwei solche übereinstimmende Gattungen bestehen, dann braucht bei Adjunction von y_1 noch nicht f_1 zu zerfallen. Hierzu ist zweierlei nothwendig. Zunächst muss K_1 intransitiv sein; denn es müssen schon die symmetrischen Functionen von weniger als n der z rational darstellbar werden; und dann muss k_2 unter der Gattung stehen, welche durch die eine Wurzel y_1 bestimmt ist; denn jene Function von k_2, welche die symmetrischen Functionen von $z_1, \cdots z_\nu$ darstellt, muss durch y_1 dargestellt werden können.

§ 592. Wir wollen durch Verbindung des eben abgeleiteten Satzes mit einem früher § 548 über Gattungsdiscriminanten bewiesenen ein Irreductibilitätstheorem aufstellen.

Bedeutet G_1 die Gruppe von $f_1(z) = 0$ und G_2 die Gruppe von $f_2(y) = 0$, dann können wir die Resultate aus § 548 verwerthen, denen zufolge die irreductiblen Theiler der Gattungsdiscriminanten von G_1 und K_1 und ebenso von G_2 und K_2 übereinstimmen. Da nun die beiden Gattungen K_1 und K_2 identisch sind, so stimmen G_1 und G_2 in den irreductiblen Factoren ihrer Gattungsdiscriminanten überein. Dies ist also eine nothwendige Bedingung dafür, dass $f_1 = 0$ durch Adjunction einer Wurzel von $f_2 = 0$ reducirt werde.

Wir wollen diese Ueberlegungen auf die zu einer Primzahl p gehörige Kreistheilungsgleichung

$$\frac{z^p-1}{z-1}=z^{p-1}+z^{p-2}+\cdots+z+1=0$$

anwenden. Jede Function irgend einer Gattung der Wurzeln ist in der Form

$$a+b\omega+c\omega^2+\cdots+d\omega^{p-1}$$

ausdrückbar, wobei ω eine primitive p^{te} Einheitswurzel bedeutet. Jeder Factor der Discriminante hat die Form

$$b(\omega^\alpha-\omega^\beta)+c(\omega^{2\alpha}-\omega^{2\beta})+\cdots+d(\omega^{(p-1)\alpha}-\omega^{(p-1)\beta});$$

folglich ist die Discriminante durch

$$\prod(\omega^\alpha-\omega^\beta)$$

d. h. auch durch p theilbar. Die Primzahl p ist also jedenfalls ein irreductibler Factor aller Gattungsdiscriminanten für die Kreistheilungsgleichung. Die Kreistheilungsgleichung kann nur dann durch Adjunction einer Wurzel y_1 der Gleichung $f_2(y)=0$ reductibel werden, wenn die Discriminante von $f_2(y)$ durch p theilbar ist*).

Einundsechzigste Vorlesung.

Radicalzahlen.

§ 593. Aus der Gesammtheit der algebraischen Zahlen heben wir eine besondere Art heraus, die wir Radicalzahlen im Rationalitätsbereiche 1 oder kürzer Radicalzahlen nennen wollen. Wir definiren sie auf folgende Art.

Wir gehen von dem aus der Einheit gebildeten natürlichen Rationalitätsbereiche $(\mathfrak{R})=(1)$ aus und erweitern ihn durch die Adjunction einer Wurzel v_ν einer reinen Gleichung oder binomischen Gleichung, deren Grad eine Primzahl p_ν ist, so dass also

$$v_\nu^{p_\nu}=F_\nu(\mathfrak{R})$$

wird. Aus dem so festgelegten Rationalitätsbereiche $(v_\nu;\mathfrak{R})$ treten wir durch fernere Adjunction einer Wurzel $v_{\nu-1}$ wieder einer reinen

*) Kronecker, Journ. de math. 19 (1854), p. 177. — Schönemann, Journ. f. Math. 32 (1846), p. 100. — Kronecker, Journ. f. Math. 100 (1887), p. 79.

Gleichung von Primzahlgrad, die auch mit der ersten zusammenfallen kann,

$$v_\nu^{p_\nu - 1} = F_{\nu-1}(v_\nu; \mathfrak{R})$$

in ein erweitertes Gebiet; $p_{\nu-1}$ bedeutet wieder eine Primzahl, und $F_{\nu-1}$ eine ganze rationale Function der Argumente; dass die Benutzung gebrochener Functionen keine Verallgemeinerung bietet, haben wir § 581 gezeigt.

In der angegebenen Weise kann man fortschreiten, bis man nach einer endlichen Anzahl von Schritten zu dem für unsere Zwecke nöthigen, völligen Schema einer Kette reiner Gleichungen von Primzahlgrad gelangt, welche die Form hat

$$(1) \qquad \begin{aligned} v_\nu^{p_\nu} &= F_\nu(\mathfrak{R}), \\ v_{\nu-1}^{p_\nu - 1} &= F_{\nu-1}(v_\nu, \mathfrak{R}), \\ v_{\nu-2}^{p_\nu - 2} &= F_{\nu-2}(v_{\nu-1}, v_\nu, \mathfrak{R}), \\ &\cdots\cdots\cdots \\ v_2^{p_2} &= F_2(v_3, v_4, \cdots v_\nu, \mathfrak{R}), \\ v_1^{p_1} &= F_1(v_2, v_3, \cdots v_\nu, \mathfrak{R}). \end{aligned}$$

Hierbei ist es nicht nöthig, dass in die Definitionsgleichung eines v_α jede vorhergehende Grösse $v_{\alpha+1}, v_{\alpha+2}, \cdots$ eingeht; sie können sogar sämmtlich fehlen.

Wir nennen jede Grösse von der Form

$$(2) \qquad x = m_0 + m_1 v_1 + m_2 v_1^2 + \cdots + m_{p_1-1} v_1^{p_1-1},$$

in welcher sämmtliche m_λ dem Bereiche $(v_2, v_3, \cdots v_\nu, \mathfrak{R})$ angehören,

$$m_\lambda = T(v_2, v_3, \cdots v_\nu, \mathfrak{R}),$$

eine zur Kette (1) gehörige Radicalgrösse, weil sie durch Adjunctionen allein von Wurzelgrössen erlangt wird. Ob nicht etwa jede algebraische Grösse zugleich eine Radicalgrösse ist, d. h. ob sich nicht etwa jede algebraische Grösse in der Form (2) darstellen lässt, gehört zu den wichtigsten und interessantesten Fragen der Algebra. Ihre Beantwortung liefert die Entscheidung über die sogenannte Auflösbarkeit der algebraischen Gleichungen, d. h. eben über die Frage, ob die Wurzeln jeder algebraischen Gleichung in der Form (2) darstellbar sind. Wir kommen hierauf bald zurück.

Die Anordnung der v in die Tabelle (1) ist nicht in allen Fällen fest bestimmt. Ist z. B. F_μ bei $\mu < \nu$ eine Function im natürlichen

Bereiche ($\mathfrak{R}$), dann kann die Gleichung für v_μ ebensogut an die erste Stelle statt der für v_ν gesetzt werden. Solche Radicale mögen **Anfangsradicale** heissen.

Es kann ferner vorkommen, dass ein Radical v_μ in keiner der folgenden Definitionsgleichungen mehr auftritt, so dass wir schreiben könnten

$$v_{\mu-1}^{p_{\mu-1}} = F_{\mu-1}(v_{\mu+1}, \cdots v_\nu, \mathfrak{R}),$$
$$v_{\mu-2}^{p_{\mu-2}} = F_{\mu-2}(v_{\mu-1}, v_{\mu+1}, \cdots v_\nu, \mathfrak{R}),$$
$$\cdots\cdots\cdots\cdots\cdots$$

dann lässt sich dieses v_μ an jede tiefere Stelle bringen, speciell auch an die letzte statt v_1. Ein solches Radical wollen wir ein **Endradical** nennen; es wird bei der Darstellung (2) nur in den Coefficienten m_λ auftreten, welche ganze Functionen dieses äusseren Radicals werden. Es ist x eine ganze Function jedes derartigen Endradicals v_μ

$$x = n_0 + n_1 v_\mu + n_2 v_\mu^2 + \cdots;$$
$$n_\lambda = T(v_1, \cdots v_{\mu-1}, v_{\mu+1}, \cdots v_\nu, \mathfrak{R}).$$

Zwischen die Anfangs- und die Endradicale ordnen sich die **Mittelradicale** ein, deren Stellung von den übrigen Gliedern abhängiger ist.

§ 594. Für unsere weiteren Entwickelungen brauchen wir einen, zuerst von **Abel** ausgesprochenen Hülfssatz*): Bedeutet p eine Primzahl, und $f_0, f_1, \cdots f_{p-1}; f$ eine Reihe von Grössen, die einem gegebenen Rationalitätsbereiche angehören, so folgt aus dem gleichzeitigen Bestehen der beiden Gleichungen

$$\text{(A)} \qquad \begin{aligned} f_0 + f_1 w + f_2 w^2 + \cdots + f_{p-1} w^{p-1} &= 0, \\ w^p - f &= 0, \end{aligned}$$

dass entweder $f_0, f_1, \cdots f_{p-1}$ einzeln verschwinden, oder dass eine der Wurzeln w der zweiten Gleichung dem Rationalitätsbereiche angehört.

Sind nämlich nicht alle Coefficienten $f_0, f_1, \cdots f_{p-1}$ gleich Null, dann haben die Polynome in (A) einen gemeinsamen Theiler, der als Divisor des zweiten Ausdruckes die Form

$$w^m - g_{m-1} w^{m-1} + \cdots \mp g_1 w \pm g_0$$

besitzt, und in dem alle g ganze Grössen des Rationalitätsbereiches sind. Die Wurzelpunkte dieses Ausdruckes sind unter den Wurzeln

*) Oeuvres, édit. **Sylow** et **Lie**, II, p. 228. — A. **Kneser**, Journ. f. Math. 106 (1890), p. 46 hat einen rein arithmetischen Beweis für diesen Satz gegeben.

von $w^p = f$ enthalten. Ist nun w_1 eine derselben, und bedeutet ω eine primitive p^{te} Einheitswurzel, dann sind alle Wurzelpunkte jenes Ausdruckes von der Form $w_1\omega^\alpha$, $w_1\omega^\beta$, $\cdots$, und deshalb wird ihr Product

$$g_0 = w_1^m \omega^\varrho.$$

Nun können wir zwei ganze Zahlen bestimmen, welche der Gleichung $mr = 1 - ps$ genügen. Erhebt man die Gleichung für g_0 in die r^{te} Potenz, dann folgt

$$g_0^r = \omega^{\varrho r} w_1^{1-ps}, \quad \omega^{\varrho r} w_1 = g_0^r f^s,$$

d. h. die Wurzel $\omega^{\varrho r} w_1$ von $w^p = f$ gehört dem Rationalitätsbereiche an.

Wir wollen uns auf diesen Hülfssatz durch dem Hinweis „nach (A)“ berufen.

Dieser Hülfssatz ist nur dann von Nutzen, wenn f von 1 verschieden, also w keine Einheitswurzel ist. Denn für $w^p = 1$ verwirklicht sich ja stets die Eventualität, dass eine der Wurzeln rational sei. Es ist deshalb von Wichtigkeit, eine genaue Unterscheidung zwischen den in (1) eingeführten Einheitswurzeln und den übrigen Radicalen zu treffen.

Wir setzen daher fest: Ist in dem Schema (1) irgend eine der eingeführten Grössen v_α durch $v_{\alpha+1}, \cdots v_\nu$ und durch irgend welche primitiven Einheitswurzeln von Primzahlgrad rational darstellbar, dann ersetzen wir die Einführung von v_α durch diejenige jener Einheitswurzeln und gestalten dadurch unser Schema um. So wird z. B. die Einführung einer durch $w^2 = 2$ definirten Radicalgrösse w durch diejenige einer primitiven achten Einheitswurzel, also durch die Einführung der Kettenglieder

$$v_1^2 = 1, \quad v_2^2 = v_1, \quad v_3^2 = v_2$$

zu ersetzen sein, da, wenn ω jene primitive 8te Einheitswurzel ist, die Irrationalität w d. h. hier

$$\sqrt{2} = \omega + \omega^7$$

wird.

Diese Umformung einer vorgelegten Kette (1) wird bei v_ν ihren Anfang zu nehmen haben, und wenn sie bis zu Ende durchgeführt ist, wird keine Beziehung zwischen den v und Einheitswurzeln

$$v_\alpha = T(v_{\alpha+1}, \cdots v_\nu, \omega', \omega'', \cdots, \mathfrak{R})$$

mehr bestehen dürfen.

Daraus können wir sofort den Schluss ziehen, dass die in (1)

zurückbleibenden Gleichungen, welche keine Einheitswurzeln definiren, irreductibel im jedesmal angegebenen Rationalitätsgebiete sind. Denn wäre eine Gleichung von der Form $v_\alpha^p = F$ nicht irreductibel, dann gäbe es eine Gleichung

$$f_0 + f_1 v_\alpha + f_2 v_\alpha^2 + \cdots = 0, \qquad f_\lambda = T(v_{\alpha+1}, \cdots v_\nu, \Re)$$

von niederem als dem p^{ten} Grade mit nicht verschwindenden Coefficienten, welche mit der ersteren eine Wurzel gemeinsam hat. Nach (A) hätte $v_\alpha^p = F$ eine rationale Wurzel; und also sind alle Wurzeln rational, wenn man eine primitive p^{te} Wurzel der 1, etwa ω_p, zum Rationalitätsgebiete rechnet; denn aus einer Wurzel von $v_\alpha^p = F$ entstehen alle übrigen durch Multiplication mit p^{ten} Einheitswurzeln. Das adjungirte v_α wäre mithin auch schon in $(\omega_p, v_{\alpha+1}, \cdots v_\nu, \Re)$ enthalten, und danach könnte die Kette der Gleichungen (1) noch vereinfacht werden.

§ 595. Ist v_1 keine Einheitswurzel, dann können wir über (2) eine Voraussetzung machen, oder dieselbe eventuell durch eine Umformung verwirklichen, welche oft von Vortheil ist. Es sei m_α einer der von 0 verschiedenen Coefficienten von (2), nur nicht m_0. Wir setzen dann die Gleichungen an

$$(3) \qquad w_1 = m_\alpha v_1^\alpha; \qquad m_\alpha = (v_2, v_3, \cdots),$$

deren zweite den Rationalitätsbereich angiebt. Es wird

$$(3^a) \qquad w_1^{p_1} = m_\alpha^{p_1} \cdot F^\alpha(v_2, v_3, \cdots) = \Phi_1(v_2, v_3, \cdots);$$

ferner bestimmen wir r und s ganzzahlig gemäss der Gleichung $\alpha r = 1 - p_1 s$; dann ist, wenn man (3) in die r^{te} Potenz erhebt,

$$(4) \qquad w_1^r = (m_\alpha^r F_1^{-s}) \cdot v_1; \quad v_1 = \frac{F_1^s}{m_\alpha^r} w_1^r = n_r w_1^r,$$

wobei $n_r = (v_2, \cdots v_\nu, \Re)$ ist. (4) giebt die Umkehrung von (3).

Trägt man (4) in (2) ein und berücksichtigt dabei das Glied $m_\alpha v_1^\alpha$ gemäss (3), dann entsteht

$$(2^a) \quad x = m_0 + w_1 + m_2' w_1^2 + \cdots + m_{p_1-1}' w_1^{p_1-1}; \qquad m_\lambda' = (v_2, v_3, \cdots),$$

also eine Darstellung, die genau den Charakter von (2) und dabei die Eigenthümlichkeit hat, dass der Coefficient von w_1^1 gleich 1 ist. An die Stelle von

$$v_1^{p_1} = F_1 \quad \text{tritt dabei} \quad w_1^{p_1} = \Phi_1.$$

Ist dagegen v_1 eine Einheitswurzel, dann kann man die besprochene Umänderung nicht ausführen, da dies gegen die Reductionsvorschriften des vorigen Paragraphen verstossen würde.

Jede der Gleichungen (1) lässt sich, wenn v_β dasjenige letzte vor $v_{\alpha-1}$ stehende Kettenglied bedeutet, welches in $F_{\alpha-1}$ wirklich vorkommt,

$$v_{\alpha-1}^{p_\alpha-1} = a_0 + a_1 v_\beta + a_2 v_\beta^2 + \cdots + a_{p_\beta-1} v_\beta^{p_\beta-1},$$

$$a_\lambda = (v_{\beta+1}, v_{\beta+2}, \cdots)$$

schreiben. Dieser Ausdruck kann nach der eben besprochenen Methode umgestaltet werden, wenn v_β keine Einheitswurzel ist. Dabei bemerken wir, dass wenn z. B. $v_{\alpha-2}^{p_\alpha-2}$ gleichfalls v_β in derselben Weise enthält,

$$v_{\alpha-2}^{p_\alpha-2} = b_0 + b_1 v_\beta + b_2 v_\beta^2 + \cdots + b_{p_\beta-1} v_\beta^{p_\beta-1},$$

mit Hervorhebung des Rationalitätsbereiches:

$$b_\lambda = (v_{\beta+1}, v_{\beta+2}, \cdots),$$

nicht in beiden Ausdrücken gleichzeitig diese Reduction gemacht werden kann.

§ 596. Wir führen für diese Vorlesung als bleibende Bezeichnung ein, dass ω_μ eine primitive p_μ^{te} Einheitswurzel sein soll.

Wenn v_1 keine Einheitswurzel ist, dann bilden wir das Product

$$(5) \qquad P(x) = \prod_{\alpha=0}^{p_1-1} [x - (m_0 + m_1 v_1 \omega_1^\alpha + m_2 v_1^2 \omega_1^{2\alpha} + \cdots)],$$

$$m_\lambda = (v_2, \cdots).$$

Da dies in $v_1, v_1\omega_1, v_1\omega_1^2, \cdots$ symmetrisch ist, so enthält es v_1 überhaupt nicht mehr, und alle die Coefficienten der Potenzen von x^{p_1}, $x^{p_1-1}, \cdots$ gehören zu $(v_2, v_3, \cdots)$.

Es ist leicht zu zeigen, dass $P(x)$ im Gebiete $(v_2, v_3, \cdots)$ irreductibel ist. Denn P ist die Norm einer linearen und also irreductiblen Function und daher nach § 584 die Potenz einer irreductiblen Function. Der zugehörige Exponent kann nur dann grösser als 1 werden, wenn für verschiedene α und β

$$m_0 + m_1 v_1 \omega_1^\alpha + m_2 v_1^2 \omega_1^{2\alpha} + \cdots = m_0 + m_1 v_1 \omega_1^\beta + m_2 v_1^2 \omega_1^{2\beta} + \cdots$$

und sonach

$$m_1 v_1 (\omega_1^\alpha - \omega_1^\beta) + m_2 v_1^2 (\omega_1^{2\alpha} - \omega_1^{2\beta}) + \cdots = 0$$

würde. Berücksichtigt man aber $v_1^{p_1} = F_1$, so würde daraus nach (A) folgen, dass entweder $v_1 = (v_2, v_3, \cdots, \omega_1)$ wird, was durch unsere Reductionsvorschriften ausgeschlossen ist, oder dass alle Coefficienten der letzten Gleichung verschwinden. Da nun die $m_1, m_2, \cdots$ nicht sämmtlich Null sind, so müsste $\alpha = \beta$ sein. Das widerspräche der Annahme $\alpha \neq \beta$. Folglich ist $P(x)$ im Bereiche $(v_2, v_3, \cdots)$ irre-

ductibel, und $P(x) = 0$ ist diejenige irreductible Gleichung dieses Bereiches $(v_2, v_3, \cdots)$, welche

$$(2) \qquad x = m_0 + m_1 v_1 + m_2 v_1^2 + \cdots + m_{p_1 - 1} v_1^{p_1 - 1}$$

als Wurzel hat.

Ist dagegen in (2) v_1 gleich einer Einheitswurzel ω_1, dann braucht das Product statt p_1 nur $(p_1 - 1)$ Factoren zu umfassen, nämlich für $\alpha = 1, 2, \cdots p_1 - 1$

$$(6) \qquad \prod_\alpha [x - (m_0 + m_1 \omega_1^\alpha + m_2 \omega_1^{2\alpha} + \cdots)]; \qquad m_\lambda = (v_2, v_3, \cdots),$$

um von ω_1 frei zu werden, wie man daraus erkennt, dass $\omega_1, \omega_1^2, \cdots$ die Wurzeln der irreductiblen Gleichung sind

$$\omega^{p_1 - 1} + \omega^{p_1 - 2} + \cdots + \omega + 1 = 0.$$

Dabei ist zugleich in diesem Falle das entstandene Product nicht nothwendig in $(v_2, \cdots)$ irreductibel, sondern es kann eine Potenz werden. Denn betrachten wir den Exponenten α und einen anderen beliebigen β, den wir $= \frac{\alpha}{\varkappa}$ schreiben können, da $\beta\varkappa \equiv \alpha \pmod{p_1}$ stets lösbar ist, so wird die Gleichung

$$(7) \qquad m_1 \omega_1^\alpha + m_2 \omega_1^{2\alpha} + \cdots = m_1 \omega_1^{\frac{1}{\varkappa}\alpha} + m_2 \omega_1^{\frac{1}{\varkappa} 2\alpha} + \cdots$$

oder

$$(m_1 - m_\varkappa)\, \omega_1^\alpha + (m_2 - m_{2\varkappa})\, \omega_1^{2\alpha} + \cdots = 0$$

stets dann befriedigt sein, wenn die Gleichungen gelten

$$m_1 = m_\varkappa, \quad m_2 = m_{2\varkappa}, \quad m_3 = m_{3\varkappa}, \quad \cdots.$$

Das kann nun, falls $\varkappa$ keine primitive Congruenzwurzel für p_1 ist, sehr wohl möglich sein, ohne dass alle m einander gleich werden. Dieser letzte Fall ist natürlich auszunehmen, da sonst schon der in (6) eingehende Factor

$$x - (m_0 + m_1 \omega_1 + m_1 \omega_1^2 + \cdots) = x - (m_0 - m_1)$$

von ω_1 frei sein würde. Man erkennt leicht, dass bei einem solchen Falle der Reductibilität in dem Ausdrucke (6) die Einheitswurzeln $\omega_1^\alpha, \omega_1^{2\alpha}, \cdots$ zu Kreistheilungsperioden angeordnet auftreten, dass also die Form entsteht (vgl. I, § 314)

$$\prod (x - [m_0 + m' \cdot (v, g^1) + m'' \cdot (v, g^2) + \cdots]).$$

Als Beispiel mag für $p_1 = 5$ die Function

$$\prod (x - [m_0 + m_1 \omega_1^\alpha + m_2 \omega_1^{2\alpha} + m_2 \omega_1^{3\alpha} + m_1 \omega_1^{4\alpha}])$$
$$= [(x - m_0)^2 + (m_1 + m_2)(x - m_0) - (m_1^2 + m_2^2 - 3 m_1 m_2)]^2$$

gelten, bei der in der That die Norm nicht irreductibel ist.

§ 597. Wir fragen jetzt, ob bei der Productbildung (5), also unter der Annahme, dass v_1 keine Einheitswurzel sei, noch ein anderes, früheres Kettenglied verschwinden kann, und zwar wollen wir zunächst untersuchen, ob neben dem Endradical v_1 noch ein anderes Endradical wegfallen kann. Nach § 593 können wir, falls dies bei einem Endradicale eintritt, dasselbe unmittelbar als v_2 in die Kette über v_1 setzen. Ordnet man x nach dem einen und nach dem anderen Radicale an, so entsteht die doppelte Form

$$x = m_0 + m_1 v_1 + m_2 v_1^2 + \cdots; \qquad m_\lambda = (v_2, v_3, \cdots),$$
$$= n_0 + n_1 v_2 + n_2 v_2^2 + \cdots; \qquad n_\lambda = (v_1, v_3, \cdots).$$

Der Voraussetzung nach wird in dem Producte

$$P(x) = \prod_\alpha (x - [m_0 + m_1 v_1 \omega_1^\alpha + m_2 v_1^2 \omega_1^{2\alpha} + \cdots]);$$
$$m_\lambda = (v_2, v_3, \cdots)$$

neben v_1 auch v_2 verschwinden, so dass die Coefficienten von $P(x)$ zu $(v_3, v_4, \cdots)$ gehören. Nun war P im Bereiche $(v_2, v_3, \cdots)$ irreductibel; die Irreductibilität gilt also um so mehr im Bereiche $(v_3, v_4, \cdots)$.

Ebenso ist das Product

$$Q(x) = \prod_\beta (x - [n_0 + n_1 v_2 \omega_2^\beta + n_2 v_2^2 \omega_2^{2\beta} + \cdots]);$$
$$n_\lambda = (v_1, v_3, \cdots)$$

im Bereiche $(v_1, v_3, \cdots)$ irreductibel, falls wir v_2 als von einer Einheitswurzel verschieden annehmen; und da Q rational in $(v_3, v_4, \cdots)$ ist, so ist es auch in diesem Bereiche irreductibel.

Die beiden in $(v_3, v_4, \cdots)$ irreductiblen Functionen $P(x)$ und $Q(x)$ haben einen und denselben Factor, nämlich den zu $\alpha = \beta = 0$ gehörigen gemeinsam. Folglich sind sie identisch; d. h. alle einzelnen Factoren des einen Ausdruckes stimmen mit denen des anderen überein, woraus dann auch $p_1 = p_2$ folgt.

Wir schreiben jetzt, um anzudeuten, das die m ganze Functionen von v_2 sind, für den ersten Factor von $P(x)$ ausführlicher

$$x - [m_0(v_2) + m_1(v_2) \cdot v_1 + m_2(v_2) \cdot v_1^2 + \cdots];$$

die Factoren von Q werden dann durch die Formel

$$x - \left[m_0\left(v_2 \omega_2^\beta\right) + m_1\left(v_2 \omega_2^\beta\right) \cdot v_1 + m_2\left(v_2 \omega_2^\beta\right) \cdot v_1^2 + \cdots\right]$$

gegeben; und da diese Factoren von Q mit denen von P übereinstimmen, so muss für ein passend gewähltes ϱ die Differenz zweier solcher Ausdrücke und deswegen auch

$$(8) \qquad \sum_{\varkappa} [m_\varkappa(v_2 \omega_2^\beta) - m_\varkappa(v_2)\, \omega_1^{\varrho\varkappa}]\, v_1^\varkappa$$

verschwinden. Verbindet man mit (8) die Definitionsgleichung $v_1^{p_1} = F_1$, so giebt (A) folgende Alternative: Entweder ist $v_1 = (v_2, v_3, \cdots, \omega_1, \omega_2) = (v_2, v_3, \cdots, \omega_1)$, was ausgeschlossen werden muss; oder es verschwinden in (8) alle einzelnen Coefficienten, was also eintritt.

Wir setzen nun, um diesen letzten Fall zu untersuchen,

$$m_\varkappa(v_2) = q_0^{(\varkappa)} + q_1^{(\varkappa)} v_2 + q_2^{(\varkappa)} v_2^2 + \cdots; \qquad q_\lambda^{(\varkappa)} = (v_3, v_4, \cdots),$$

dann giebt das eben erhaltene Resultat, da $\omega_1 = \omega_2$ wegen $p_1 = p_2$ genommen werden kann, für $\beta = 1$ und für ein passendes ϱ die Gleichung

$$q_0^{(\varkappa)}(1 - \omega_1^{\varrho\varkappa}) + q_1^{(\varkappa)}(\omega_1 - \omega_1^{\varrho\varkappa})\, v_2 + q_2^{(\varkappa)}(\omega_1^2 - \omega_1^{\varrho\varkappa})\, v_2^2 + \cdots = 0.$$

Wegen $v_2^{p_1} = (v_3, \cdots)$ und der Unmöglichkeit von $v_2 = (v_3, \cdots \omega_1)$ liefert (A) das Ergebniss, dass in der letzten Gleichung alle Coefficienten verschwinden. Da aber die in dieser Gleichung auftretenden Klammern i. A. nicht verschwinden, so folgt, dass nur $q_{\varrho\varkappa}^{(\varkappa)}$ von Null verschieden sein kann, wobei wie gewöhnlich der untere Index auf seinen kleinsten nicht negativen Rest mod. p_1 zu reduciren wäre.

Hiernach erhalten wir den einfachen Ausdruck

$$m_\varkappa(v_2) = q_{\varrho\varkappa} v_2^{\varrho\varkappa}; \qquad q_\lambda = (v_3, v_4, \cdots);$$

der jetzt unnöthige obere Index des q ist hier fortgelassen. Daraus folgt durch Substitution dieses Werthes in (2)

$$x = q_0 + q_\varrho \cdot (v_1 v_2^\varrho) + q_{2\varrho} \cdot (v_1 v_2^\varrho)^2 + \cdots.$$

Wenn man deshalb, statt nach einander v_2 und dann v_1 einzuführen, die Grösse $w_2 = v_1 v_2^\varrho$ durch die Definitionsgleichung

$$w_2^{p_1} = F_1(v_3, \cdots) \cdot F_2^\varrho(v_3, \cdots)$$

einführt, dann kommt man zu einer vereinfachten Kette von Radicalgrössen, welche hinsichtlich der Darstellung von x dasselbe leistet, wie (1). Denkt man sich diese Vereinfachungen von vornherein durchgeführt, was natürlich erst geschehen kann, wenn x vorliegt, dann ist bei der Productbildung (5) das Verschwinden zweier Endradicale, unter denen keine Einheitswurzel sich befindet, ausgeschlossen.

Wir fügen daher den Bedingungen aus § 594 über die Reduction der Kette noch hinzu, dass es nicht möglich sein soll, ohne Verletzung der bisherigen Festsetzungen bei der ersten Productbildung (5) und den weiteren Productbildungen

(§ 585) durch andere Wahl der Definitionsgleichungen die Anzahl der Kettenglieder zu vermindern.

Ist hingegen eine der Grössen v_1 und v_2, oder sind sie beide Einheitswurzeln, dann ist es möglich, dass sie gleichzeitig bei der Productbildung (5) fortfallen. Man erkennt leicht, dass im ersten Falle, wenn $v_2 = \omega_2$ ist, $(p_1 - 1)$ ein Vielfaches von p_2 werden muss; und dass im zweiten Falle $v_1 = \omega_1$, $v_2 = \omega_2$ Kreistheilungsperioden von $\frac{p_1 - 1}{\lambda}$ und $\frac{p_2 - 1}{\lambda}$ Gliedern in Combination auftreten. Die folgenden Beispiele geben Belege hierfür.

$$p_1 = 5; \quad v_1 = \omega_1; \quad v_2^2 = q.$$

$$x = \sqrt{q}\,\omega_1 - \sqrt{q}\,\omega_1^2 - \sqrt{q}\,\omega_1^3 + \sqrt{q}\,\omega_1^4;$$

$$P(x) = \prod_{\alpha=1}^{4} [x - \sqrt{q}\,(\omega_1^\alpha + \omega_1^{4\alpha}) + \sqrt{q}\,(\omega_1^{2\alpha} + \omega_1^{3\alpha})] = (x^2 - 5q)^2,$$

so dass bei der Productbildung v_1 und v_2 wegfallen.

Aehnlich gestaltet es sich bei

$$p_1 = 5; \quad v_1 = \omega_1; \quad p_2 = 7; \quad v_2 = \omega_2.$$

$$x = (\omega_2 + \omega_2^2 + \omega_2^4)(\omega_1 + \omega_1^4) - (\omega_2^3 + \omega_2^6 + \omega_2^5)(\omega_1^2 + \omega_1^3);$$

$$P(x) = \prod_{\alpha=1}^{4} [x - (\omega_2 + \omega_2^2 + \omega_2^4)(\omega_1^\alpha + \omega_1^{4\alpha}) - (\omega_2^3 + \omega_2^6 + \omega_2^5)(\omega_1^{2\alpha} + \omega_1^{3\alpha})]$$
$$= (x^2 - x + 9)^2,$$

wo v_1 und v_2 als Einheitswurzeln angenommen sind.

§ 598. Wir gehen jetzt zu der Untersuchung über, ob bei der Productbildung (5) mit v_1 zugleich das unmittelbar vorhergehende Anfangs- oder Mittelradical v_2 wegfallen kann. Hierbei kann v_1 selbstverständlich keine Einheitswurzel sein, denn eine solche wäre ein Anfangsradical und könnte als solches nicht von v_2 abhängen. Ebenso soll v_2 von einer Einheitswurzel verschieden sein.

Wir setzen

$$v_1^{p_1} = F_1^{p_1} = a_0 + a_1 v_2 + a_2 v_2^2 + \cdots; \qquad a_\lambda = (v_3, v_4, \cdots)$$

und gehen nun auf die Norm

$$(5) \qquad P(x) = \prod_{\varrho=0}^{p_1-1} [x - (m_0 + m_1 v_1 \omega_1^\varrho + m_2 v_1^2 \omega_1^{2\varrho} + \cdots)],$$
$$m_\lambda = (v_2, \cdots)$$

zurück; diese kann nur dadurch von v_2 frei werden, dass in dem ausgeführten Producte auf der rechten Seite lediglich die Potenzen v_2^0, $v_2^{p_2}$, $v_2^{2p_2}$, $\cdots$ auftreten, für welche dann ja $1, F_2, F_2^2, \cdots$ eingetragen

werden darf. $P(x)$ ändert sich daher nicht, wenn in $(m_0 + m_1 v_1 + \cdots)$ überall v_2 durch $v_2 \omega_2^\alpha$ mit beliebigem Exponenten α ersetzt wird. Wir wollen die Werthe, welche dadurch an die Stelle von $m_0, m_1, m_2, \cdots; v_1$ treten, mit

$$m_{0\alpha}, \; m_{1\alpha}, \; m_{2\alpha}, \cdots; \; v_{1\alpha}$$

bezeichnen, so dass man auch statt (5) hat

$$(9) \quad P(x) = \prod_{\varrho=0}^{p_1-1} \left[x - \left(m_{0\alpha} + m_{1\alpha} v_{1\alpha} \omega_1^\varrho + m_{2\alpha} v_{1\alpha}^2 \omega_1^{2\varrho} + \cdots\right)\right];$$
$$m_{\lambda\alpha} = (v_2 \omega_2^\alpha, v_3, \cdots).$$

Da v_1 keine Einheitswurzel ist, so können wir hier den Coefficienten m_1 und also $m_{1\alpha}$ gleich 1 setzen (§ 595).

Die einzelnen Wurzeln in (5) stimmen mit denen in (9) überein; demnach gilt für passend gewählte $\varrho, \sigma, \cdots$ das System von p_1 Gleichungen

$$m_{0\alpha} + v_{1\alpha} \quad + m_{2\alpha} v_{1\alpha}^2 \quad + \cdots = m_0 + v_1 \omega_1^\varrho + m_2 v_1^2 \omega_1^{2\varrho} + \cdots,$$
$$(10) \quad m_{0\alpha} + v_{1\alpha} \omega_1 + m_{2\alpha} v_{1\alpha}^2 \omega_1^2 + \cdots = m_0 + v_1 \omega_1^\sigma + m_2 v_1^2 \omega_1^{2\sigma} + \cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

wobei die Exponenten $\varrho, \sigma, \cdots$ der rechten Seiten bis auf ihre Folge den Zahlen $0, 1, 2, \cdots (p_1 - 1)$ gleich sein werden. Aus (10) folgt durch Combination der Gleichungen der Werth von $v_{1\alpha}$ in der Form

$$(11) \quad v_{1\alpha} = n_{0\alpha} + n_{1\alpha} v_1 + n_{2\alpha} v_1^2 + \cdots; \qquad n_{\lambda\alpha} = (v_2, v_3, \cdots \omega_1).$$

Durch Potenzirung möge sich aus (11) ergeben

$$v_{1\alpha}^{p_1} = F_1(v_2 \omega_2^\alpha, v_3, \cdots) = (n_{0\alpha} + n_{1\alpha} v_1 + n_{2\alpha} v_1^2 + \cdots)^{p_1}$$
$$= N_{0\alpha} + N_{1\alpha} v_1 + N_{2\alpha} v_1^2 + \cdots,$$
$$N_{\lambda\alpha} = (v_2, v_3, \cdots \omega_1).$$

Mit dieser Gleichung für v_1 verbinden wir die Definitionsgleichung $v_1^{p_1} = F_1$ und schliessen nach (A), dass entweder $v_1 = (v_2, v_3, \cdots \omega_1, \omega_2)$ ist, oder dass die $N_{1\alpha}, N_{2\alpha}, \cdots$ sämmtlich verschwinden. Das Erste ist wegen der Vorschriften über die Reduction von (1) ausgeschlossen; folglich ist jedes $N_{\lambda\alpha} = 0$ für $\lambda = 1, 2, \cdots$, und demnach

$$v_{1\alpha}^{p_1} = N_{0\alpha} = (v_2, v_3, \cdots \omega_1)$$

von v_1 unabhängig. Eine Umänderung in (11) von v_1 in $v_1 \omega_1$ kann, da hierbei $v_{1\alpha}^{p_1}$ ungeändert bleibt, dem $v_{1\alpha}$ höchstens einen Factor $\omega_1^\varkappa$ anfügen, d. h. man hat

$$(12) \qquad v_{1\alpha} \omega_1^\varkappa = n_{0\alpha} + n_{1\alpha} v_1 \omega_1 + n_{2\alpha} v_1^2 \omega_1^2 + \cdots.$$

Durch Combination von (11) und (12) ergiebt sich

$$n_{0\alpha}(\omega_1^{\varkappa}-1)+n_{1\alpha}(\omega_1^{\varkappa}-\omega_1)v_1+n_{2\alpha}(\omega_1^{\varkappa}-\omega_1^2)v_1^2+\cdots=0$$

und daraus in bekannter Weise nach (A), dass alle $n_{\lambda\alpha}$ mit Ausnahme von $n_{\varkappa\alpha}$ verschwinden. Man darf demnach statt (11) die vereinfachte Form ansetzen

$$v_{1\alpha}=n_{\varkappa\alpha}v_1^{\varkappa}; \qquad n_{\varkappa\alpha}=(v_2, v_3, \cdots v_\nu;\ \omega_1).$$

Diese tragen wir in die erste der Gleichungen (10) ein und beachten, dass $\varkappa, 2\varkappa, 3\varkappa, \cdots$ nach dem Modul p_1 mit $1, 2, 3, \cdots$ bis auf die Folge übereinstimmen; dann ergiebt wieder der Abel'sche Hülfssatz (A) das Resultat:

$$(13)\qquad v_{1\alpha}=m_\varkappa v_1^{\varkappa}\omega_1^{\varrho\varkappa},$$

$$(14)\qquad v_{1\alpha}^{p_1}=m_\varkappa^{p_1}v_1^{\varkappa p_1}, \qquad m_\varkappa=(v_2,\cdots v_\nu).$$

Gleichzeitig wird ersichtlich, dass, weil jeder der Exponenten $1, 2, \cdots p_1-1$ von v_1 rechts und links in (10) je einmal auftritt, die einzelnen Glieder, welche durch Potenzirung der Summanden in (10) entstehen,

$$(15)\qquad v_1^{p_1},\quad (m_2v_1^2)^{p_1},\quad (m_3v_1^3)^{p_1},\ \cdots$$

durch die Einführung von $\omega_2^\alpha v_2$ an Stelle von v_2 nur in einander übergehen. Dabei ist es nicht möglich, dass zwei verschiedene Exponenten α und β von ω_2 die gleiche Umstellung der Glieder von (15) unter einander hervorbringen. Denn sonst müssten zwei Ausdrücke aus (15), welche die Form haben

$$(16)\qquad d_0+d_1v_2\omega_2^\alpha+d_2v_2^2\omega_2^{2\alpha}+\cdots \quad\text{und}\quad d_0+d_1v_2\omega_2^\beta+d_2v_2^2\omega_2^{2\beta}+\cdots,$$
$$(\alpha \gtrless \beta)$$

einander gleich sein. Die $d_1, d_2, \cdots$ können nicht sämmtlich verschwinden, weil sonst $v_1^{p_1}$ von v_2 unabhängig wäre; ferner kann nicht $v_2=(v_3,\cdots,\omega_1,\omega_2)$ sein; folglich zeigt (A), dass $\alpha=\beta$ wird, entgegen der Annahme $\alpha \gtrless \beta$.

Die besprochene Umwandlung in der Folge der Glieder von (15) können wir folgendermassen bequem darstellen. Geht durch Einführung von ω_2^α der Term $v_1^{p_1}$ in $(m_\varkappa v_1^\varkappa)^{p_1}$ über, so wird die nochmalige Einführung von ω_2^α das $v_1^{\varkappa p_1}$ abgesehen vom zugehörigen m in $v_1^{\varkappa\varkappa p_1}$ umwandeln; das Gleiche geschieht also bei der sofortigen Einführung von $v_2\omega_2^{2\alpha}$ statt v_2. Da nun p_2 eine Primzahl ist, so können wir eine primitive Congruenzwurzel e für p_1 annehmen, und wollen für den Augenblick unter $[\alpha]$ den kleinsten positiven Rest von e^α mod. (p_1-1) verstehen. Wir setzen bei diesen Annahmen

$$v_1 = R_0^{\frac{1}{p_1}}, \quad m_\varepsilon v_1^\varepsilon = R_1^{\frac{1}{p_1}}, \quad m_{[2]} v_1^{[2]} = R_2^{\frac{1}{p_1}}, \cdots$$

und schreiben mit unserer neuen Bezeichnung statt (2) die Form für die Grösse x

$$x = m_0 + R_0^{\frac{1}{p_1}} + R_1^{\frac{1}{p_1}} + R_2^{\frac{1}{p_1}} + \cdots + R_{p_1-2}^{\frac{1}{p_1}}. \tag{17}$$

Führt dann die Eintragung von $v_2 \omega_2^\alpha$ statt v_2 etwa R_0 in $R_\varkappa$ über, dann wird jedes R_β hierdurch in $R_{\beta+\varkappa}$ umgewandelt. Ebenso liefert die Eintragung von $v_2 \omega_2^{\mu\alpha}$ statt v_2 die Umwandlung von R_β in $R_{\beta+\mu\varkappa}$ für jedes μ und jedes β. Dabei sind die Indices der R natürlich nur mod. $(p_1 - 1)$ zu betrachten, so dass

$$R_\alpha = R_\beta \quad \text{bei} \quad \alpha \equiv \beta \pmod{(p_1 - 1)}$$

zu setzen ist.

Wir wollen jetzt unter $\varkappa$ den kleinsten Index der von R_0 aus durch Umwandlung von v_2 in $v_2 \omega_2$, $v_2 \omega_2^2, \cdots$ erreichbaren R verstehen; dann werden von R_0 aus überhaupt nur die p_2 von einander verschiedenen Werthe

$$R_0, \; R_\varkappa, \; R_{2\varkappa}, \cdots R_{(p_2-1)\varkappa} \tag{18}$$

erreichbar sein.

Alle in (18) auftretenden Indices sind verschieden und kleiner als $(p_1 - 1)$. Denn wäre etwa

$$\alpha\varkappa < p_1 - 1 < (\alpha + 1)\varkappa,$$

dann folgte daraus weiter

$$\varkappa > (\alpha + 1)\varkappa - (p_1 - 1) > 0,$$

so dass der Rest von $(\alpha + 1)\varkappa$ mod. $(p_1 - 1)$ auf einen Index führte, der noch unter $\varkappa$ läge; das war aber ausgeschlossen. Da ferner $R_{p_2\varkappa} = R_0$ wird, weil $\omega_2^{p_2} = 1$ ist, so ergiebt sich

$$p_2 \cdot \varkappa = p_1 - 1, \tag{19}$$

d. h.: Verschwindet bei der Productbildung (5) das Mittelradical v_2 zugleich mit dem Endradical v_1, wobei v_1 und v_2 keine Einheitswurzeln sind, dann ist p_2 ein Theiler von $(p_1 - 1)$.

Aus (14) kann man einen weiteren Schluss ziehen. Schreibt man beide Seiten ausführlicher in der Form

$$a_0 + a_1 v_2 \omega_2^\alpha + a_2 v_2^2 \omega_2^{2\alpha} + \cdots = d_0 + d_1 v_2 + d_2 v_2^2 + \cdots$$

und bedenkt, dass die $a_1, a_2, \cdots$ nicht sämmtlich verschwinden können, weil v_2 der Annahme nach in $v_1^{p_1}$ auftritt, dann giebt (A) entweder

$v_2 = (v_3, \cdots \omega_1, \omega_2)$, was auszuschliessen ist, oder, was also wirklich eintritt,

$$a_1 \omega_2^\alpha = d_1, \quad a_2 \omega_2^{2\alpha} = d_2, \cdots; \qquad a_\lambda \text{ und } d_\lambda = (v_3, v_4, \cdots).$$

Demnach gehört ω_2 selbst dem Rationalitätsbereiche $(v_3, v_4, \cdots)$ an. Wäre nun

$$\omega_2 = e_0 + e_1 v_\varrho + e_2 v_\varrho^2 + \cdots; \qquad e_\lambda = (v_{\varrho+1}, v_{\varrho+2}, \cdots),$$

wobei also v_ϱ das niedrigste, wirklich in ω_2 eintretende Radical ist, dann liefert (A) wieder, da $e_1 = 0$, $e_2 = 0, \cdots$ unmöglich ist, $v_\varrho = (\omega_2, v_{\varrho+1}, \cdots)$. Das ist gleichfalls nach unseren Reductionsvorschriften nicht der Fall, wenn nicht $v_\varrho = \omega_2$ wird. Mit dieser Annahme ist $p_2 = 2$ stets verträglich, weil dafür bereits $\omega_2 = -1$ innerhalb $(\mathfrak{R}) = (1)$ vorhanden ist. —

§ 599. Wir wollen nunmehr auf die zu Anfang des vorigen Paragraphen zurückgestellte Voraussetzung $v_2 = \omega_2$ eingehen. Dann bleibt also (5) ungeändert, wenn v_2 durch v_2^α ersetzt wird ($\alpha = 1, 2, \cdots p_2 - 1$). Die Aenderung, welche dadurch m_λ und v_1 erfahren, machen wir wieder durch die Bezeichnung $m_{\lambda\alpha}$, $v_{1\alpha}$ kenntlich. Die Schlussfolgerungen, welche an (10), (11), (13) geknüpft sind, bleiben ungeändert. Insbesondere gilt auch hier (13) und (14). Dagegen liefert jetzt (16) ein anderes Resultat. Hier haben wir

$$(20) \qquad d_0 + d_1 \omega_2^\alpha + d_2 \omega_2^{2\alpha} + \cdots = d_0 + d_1 \omega_2^\beta + d_2 \omega_2^{2\beta} + \cdots$$

zu betrachten, und wie sich schon bei (7) gezeigt hat, ist die Erfüllung dieser Gleichung wohl möglich, ohne dass alle $d_1, d_2, \cdots$ einander gleich werden. Der Grund dieser Verschiedenheit liegt darin, dass (A) nicht verwendet werden kann.

Die Form (17) bleibt wieder bestehen; die daran geknüpfte Umwandlung von R_0 muss aber folgendermassen abgeändert werden. Es sei g eine primitive Congruenzwurzel für p_2. Wir ersetzen $v_2 = \omega_2$ durch ω_2^g und erreichen dadurch die Umwandlung von R_0 etwa in $R_\varkappa$; dieselbe Aenderung zum zweiten Male ausgeführt liefert von $R_\varkappa$ aus $R_{2\varkappa}$; das entspricht also der Einführung von $\omega_2^{g \cdot g}$ für ω_2 in R_0. So fahren wir fort bis zur $(p_2 - 2)^{\text{ten}}$ Potenz von g. Die $(p_2 - 1)^{\text{te}}$ Potenz liefert wieder ω_2, also bleibt R_0 ungeändert. Man erhält demnach an Stelle von (18) die Reihe der von R_0 aus erreichbaren Glieder in der Form

$$(21) \qquad R_0, \ R_\varkappa, \ R_{2\varkappa}, \ \cdots \ R_{(p_2-2)\varkappa}.$$

Auch hier sind alle Indices kleiner als $(p_1 - 1)$. Folglich tritt an die Stelle von (19) hier

$$(22) \qquad (p_2 - 1)\varkappa = p_1 - 1;$$

d. h. verschwindet mit v_1 gleichzeitig bei der Productbildung (5) das Radical $v_2 = \omega_2$, dann ist $(p_2 - 1)$ ein Theiler von $(p_1 - 1)$.

Als Beispiel hierzu möge Folgendes dienen. Es sei definirt

$$v_2^3 = 1; \quad v_1^3 = 1 + v_2, \quad \text{also} \quad p_2 = p_1 = 3,$$

und wir nehmen

$$x = v_1 - v_2 \cdot v_1^2.$$

Dann wird das Product (5) hier

$$(x - v_1 + v_2 v_1^2)(x - v_1\omega_1 + v_2 v_1^2 \omega_1^2)(x - v_1\omega_1^2 + v_2 v_1^2 \omega_1)$$
$$= x^3 - 3x - 1,$$

so dass also mit v_1 gleichzeitig v_2 verschwunden ist.

§ 600. Wir wollen jetzt einen Schritt weiter gehen und annehmen, dass bei der Productbildung (5) mit v_1 zugleich die beiden unmittelbar vorhergehenden Mittelradicale v_2 und v_3 verschwinden; es kann übrigens v_2 dabei auch ein Anfangsradical sein.

Wir setzen für F_1 und für F_2 ausführlicher

$$v_1^{p_1} = a_0 + v_2 + a_2 v_2^2 + \cdots; \qquad a_\lambda = (v_3, v_4, \cdots),$$
$$v_2^{p_2} = b_0 + v_3 + b_2 v_3^2 + \cdots; \qquad b_\lambda = (v_4, v_5, \cdots).$$

Verwandelt man v_3 in $v_3\omega_3^\alpha$, so soll die linke Seite der letzten Gleichung mit $v_{2\alpha}^{p_2}$ bezeichnet werden. Ebenso wollen wir mit $a_{\lambda\alpha}$ das durch die gleiche Substitution aus a_λ entstehende Resultat bezeichnen, so dass wir schreiben

$$v_{2\alpha}^{p_2} = b_0 + v_3\omega_3^\alpha + b_2 v_3^2 \omega_3^{2\alpha} + \cdots,$$
$$a_{\lambda\alpha} = R(v_3\omega_3^\alpha, v_4, \cdots), \quad \text{wenn} \quad a_\lambda = R(v_3, v_4, \cdots).$$

Trägt man diese Grössen in die Definitionsgleichung für $v_1^{p_1}$ ein und fügt gleichzeitig dem $v_{2\alpha}$ noch den Factor ω_2^β hinzu, so entstehe die neue Form

$$v_{1\alpha\beta}^{p_1} = a_{0\alpha} + v_{2\alpha}\omega_2^\beta + a_{2\alpha} v_{2\alpha}^2 \omega_2^{2\beta} + a_{3\alpha} v_{2\alpha}^3 \omega_2^{3\beta} + \cdots.$$

Falls nun in dem früher betrachteten Producte

$$(5) \qquad P(x) = \prod_{\varrho=0}^{p_1-1} [x - (m_0 + m_1 v_1 \omega_1^\varrho + m_2 v_1^2 \omega_1^{2\varrho} + \cdots)]$$
$$m_\lambda = (v_2, v_3, \cdots)$$

mit v_1 zugleich v_2 und v_3 wegfallen, dann ändert sich P nicht, wenn

man auf der rechten Seite $v_3 \omega_3^\alpha$ statt v_3 einführt und dann ausserdem noch $v_{2\alpha}$ in $v_{2\alpha}\omega_2^\beta$ umwandelt; α und β sind dabei ganz beliebig. Geht hierdurch m_λ in

$$m_{\lambda\alpha\beta} = \left(v_{2\alpha}\omega_2^\beta,\ v_3\omega_3^\alpha,\ v_4,\cdots\right)$$

über, so können wir auch

$$(9^a)\qquad P(x) = \prod_{\varrho=0}^{p_1-1}\left[x - \left(m_{0\alpha\beta} + m_{1\alpha\beta}v_{1\alpha\beta}\omega_1^\varrho + m_{2\alpha\beta}v_{1\alpha\beta}^2\omega_1^{2\varrho} + \cdots\right)\right]$$

setzen. Da v_1 keine Einheitswurzel sein kann, so lässt sich von vornherein die Voraussetzung $m_1 = m_{1\alpha\beta} = 1$ verwirklichen. Die einzelnen Wurzeln in (5) stimmen mit denen in (9ª) überein, da in (5) die beiden Grössen v_2, v_3 keinen Einfluss ausüben. Demnach wird für passend gewählte $\varrho, \sigma, \cdots$ das System von p_1 Gleichungen bestehen

$$(10^a)\qquad \begin{aligned} m_{0\alpha\beta} + v_{1\alpha\beta} + m_{2\alpha\beta}v_{1\alpha\beta}^2 + \cdots &= m_0 + v_1\omega_1^\varrho + m_2 v_1^2\omega_1^{2\varrho} + \cdots,\\ m_{0\alpha\beta} + v_{1\alpha\beta}\omega_1 + m_{2\alpha\beta}v_{1\alpha\beta}^2\omega_1^2 + \cdots &= m_0 + v_1\omega_1^\sigma + m_2 v_1^2\omega_1^{2\sigma} + \cdots,\\ \cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

wobei die Exponenten $\varrho, \sigma, \cdots$ der rechten Seiten bis auf ihre Anordnung mit den Zahlen $0, 1, 2, \cdots (p_1 - 1)$ übereinstimmen. Aus (10ª) folgt zunächst durch Combination der Gleichungen der Werth von $v_{1\alpha\beta}$ in der Form

$$(11^a)\qquad v_{1\alpha\beta} = n_{0\alpha\beta} + n_{1\alpha\beta}v_1 + n_{2\alpha\beta}v_1^2 + \cdots;\qquad n_{\lambda\alpha\beta} = (v_2, v_3, \cdots; \omega_1).$$

Durch Potenzirung möge sich dann aus (11ª) ergeben

$$\begin{aligned} v_{1\alpha\beta}^{p_1} &= F_1\left(v_{2\alpha}\omega_2^\beta,\ v_3\omega_3^\alpha,\ v_4,\cdots\right)\\ &= \left(n_{0\alpha\beta} + n_{1\alpha\beta}v_1 + n_{2\alpha\beta}v_1^2 + \cdots\right)^{p_1}\\ &= N_{0\alpha\beta} + N_{1\alpha\beta}v_1 + N_{2\alpha\beta}v_1^2 + \cdots;\qquad N_{\lambda\alpha\beta} = (v_2, v_3, \cdots; \omega_1). \end{aligned}$$

Wie leicht zu sehen ist, können wir hieraus noch nicht wie an der entsprechenden Stelle des § 598 schliessen, dass $N_{1\alpha\beta} = 0$, $N_{2\alpha\beta} = 0, \cdots$ sei. Hier verfahren wir folgendermassen: Die letzte Gleichung setzt sich auf Grund der Definitionsgleichung für $v_{1\alpha\beta}$ in

$$a_{0\alpha} + v_{2\alpha}\omega_2^\beta + a_{2\alpha}v_{2\alpha}^2\omega_2^{2\beta} + \cdots = N_{0\alpha\beta} + N_{1\alpha\beta}v_1 + N_{2\alpha\beta}v_1^2 + \cdots$$

um; tragen wir hierin $\beta = 0, 1, \cdots (p_2 - 1)$ ein, so erhalten wir ein System, welches dem Systeme (10ª) entsprechend gebaut ist und auch ähnliche Folgerungen zulässt, die zu dem Ergebnisse

$$(23^a)\qquad v_{2\alpha} = q_{0\alpha} + q_{1\alpha}v_1 + q_{2\alpha}v_1^2 + \cdots;\qquad q_{\lambda\alpha} = (v_2, v_3, \cdots; \omega_1, \omega_2)$$

führen. Erhebt man dies in die p_2^{te} Potenz, so ergiebt sich

$$b_0 + v_3\omega_3^\alpha + b_2 v_3^2\omega_3^{2\alpha} + \cdots = Q_{0\alpha} + Q_{1\alpha}v_1 + \cdots$$
$$Q_{\lambda\alpha} = (v_2, v_3, \cdots; \omega_1, \omega_2).$$

Jetzt lassen sich die Schlüsse verwenden, welche an (11) des § 598 geknüpft wurden. Sie zeigen, dass $Q_{1\alpha} = 0$, $Q_{2\alpha} = 0, \cdots$ werden, dass folglich $v_{2\alpha}^{p_1} = Q_{0\alpha}$ von v_1 unabhängig, und also

$$(23^b) \qquad v_{2\alpha}\omega_2^\varkappa = q_{0\alpha} + q_{1\alpha}v_1\omega_1 + q_{2\alpha}v_1^2\omega_1^2 + \cdots$$

ist; und es folgt endlich, wenn man (23^a) und (23^b) vergleicht, dass auch

$$q_{0\alpha}(\omega_2^\varkappa - 1) + q_{1\alpha}(\omega_2^\varkappa - \omega_1)v_1 + q_{2\alpha}(\omega_2^\varkappa - \omega_1^2)v_1^2 + \cdots = 0$$

wird. Weil nun in (5) v_2 wegfallen sollte, so ist nach dem Hauptergebniss des vorigen Paragraphen p_2 ein Theiler von $(p_1 - 1)$; und daher ist kein $\omega_2^\varkappa = \omega_1^\lambda$, ausser wenn $\varkappa = \lambda = 0$ wird. Nach (A) schliesst man mithin $\varkappa = \lambda = 0$; $q_{1\alpha} = 0$, $q_{2\alpha} = 0, \cdots$, und weiter nach den bisher benutzten Principien aus (23^a) der Reihe nach

$$v_{2\alpha} = q_{0\alpha} = r_{0\alpha} + r_{1\alpha}v_2 + r_{2\alpha}v_2^2 + \cdots; \qquad r_{\lambda\alpha} = (v_3, v_4, \cdots; \omega_1, \omega_2),$$
$$b_0 + v_3\omega_3^\alpha + b_2 v_3^2\omega_3^{2\alpha} + \cdots = v_{2\alpha}^{p_1} = R_{0\alpha} + R_{1\alpha}v_2 + \cdots;$$
$$R_{\lambda\alpha} = (v_3, v_4, \cdots; \omega_1, \omega_2);$$
$$R_{1\alpha} = 0, \quad R_{2\alpha} = 0, \quad \cdots; \quad v_{2\alpha}^{p_1} = R_{0\alpha};$$
$$v_{2\alpha}\omega_2^\lambda = r_{0\alpha} + r_{1\alpha}v_2\omega_2 + r_{2\alpha}v_2^2\omega_2^2 + \cdots;$$
$$r_{0\alpha}(\omega_2^\lambda - 1) + r_{1\alpha}(\omega_2^\lambda - \omega_2)v_2 + r_{2\alpha}(\omega_2^\lambda - \omega_2^2)v_2^2 + \cdots = 0;$$
$$(23) \qquad v_{2\alpha} = r_{\lambda\alpha}v_2^\lambda.$$

Tragen wir dies in die oben hergeleitete Gleichung

$$v_{1\alpha\beta}^{p_1} = a_{0\alpha} + v_{2\alpha}\omega_2^\beta + a_{2\alpha}v_{2\alpha}^2\omega_2^{2\beta} + \cdots = N_{0\alpha\beta} + N_{1\alpha\beta}v_1 + N_{2\alpha\beta}v_1^2 + \cdots$$

ein, dann können wir jetzt die Schlüsse ziehen, welche vorher bei (11^a) noch nicht möglich waren, weil $v_{2\alpha}$ kein dem v_1 vorhergehendes Mittelradical war. Diese Schwierigkeit ist jetzt fortgefallen, und so findet man nach (A)

$$N_{1\alpha\beta} = 0, \quad N_{2\alpha\beta} = 0, \quad \cdots;$$
$$v_{1\alpha\beta}^{p_1} = N_{0\alpha\beta};$$

und also unter Benutzung der Gleichung (11^a)

$$v_{1\alpha\beta}\omega_1^\tau = n_{0\alpha\beta} + n_{1\alpha\beta}v_1\omega_1 + n_{2\alpha\beta}v_1^2\omega_1^2 + \cdots;$$
$$n_{0\alpha\beta}(\omega_1^\tau - 1) + n_{1\alpha\beta}(\omega_1^\tau - \omega_1)v_1 + n_{2\alpha\beta}(\omega_1^\tau - \omega_1^2) + \cdots = 0,$$
$$(24) \qquad v_{1\alpha\beta} = n_{\tau\alpha\beta}v_1^\tau.$$

Trägt man die Resultate (23) und (24) in (10^a) ein, dann stehen links ausser den ω auch nur Grössen $v_1, v_2, v_3, \cdots$, und nach (A) wird es ersichtlich, dass die einzelnen Glieder links den einzelnen Gliedern rechts gleich sind. Insbesondere ist also zu setzen

$$(25) \qquad v_{1\alpha\beta} = m_\tau v_1^\tau \omega_1^{\varrho\tau}.$$

Wir gehen jetzt auf die Gleichung (23) zurück. Diese zeigt uns, dass bis auf einen in $(v_3, v_4, \cdots; \omega_1, \omega_2)$ rationalen Factor $r_{\lambda\alpha}$ durch die Substitution von $v_3\omega_3^\alpha$ statt v_3 die Grösse v_2 in v_2^λ übergeht. Macht man nun in der Definitionsgleichung von $v_{2\alpha}^{p_2}$ dieselbe Substitution, so erhält man $v_{2,2\alpha}$, und dies ist demnach bis auf einen solchen in $(v_3, v_4, \cdots; \omega_1, \omega_2, \omega_3)$ rationalen Factor gleich $v_2^{\lambda^2}$. Ebenso zeigt sich allgemein, dass $v_{2,\sigma\alpha}$ bis auf einen in $(v_3, v_4, \cdots; \omega_1, \omega_2, \omega_3)$ rationalen Factor mit der $(\lambda^\sigma)^{\text{ten}}$ Potenz von v_2 übereinstimmt. Nehmen wir $\sigma = p_3$, dann muss $\lambda^{p_3} \equiv 1 \pmod{p_2}$ sein, weil $v_{2,p_3\alpha} = v_2$ wird; d. h. der Exponent p_3 ist ein Theiler von $(p_2 - 1)$.

Natürlich ist hierbei zu beachten, dass $v_2^{p_2}$ wirklich eine Function von v_3 sein muss, wie das ja durch die Form der Definitionsgleichung auch angedeutet wurde; das Gleiche gilt für (23).

Sind v_2 und v_3 zwei Mittelradicale, von denen jedes einzelne unmittelbar in das Kettenschema vor v_1 gestellt werden kann, dann gelten von v_3 die im § 598 für v_2 gefundenen Resultate.

§ 601. Da jedes Kettenglied, welches in der Reihe der Definitionsgleichungen als Endradical auftritt, an die letzte Stelle gesetzt werden kann, so gilt bei einer nach einem solchen Endradical vorgenommenen Normbildung Alles, was bisher über v_1 abgeleitet ist. Bei der Herstellung von Normen hingegen, welche nicht an Endradicale anknüpfen, werden die bisherigen Theoreme ungültig.

Wir wollen dies an dem Beispiele der Gleichungen vierten Grades zeigen. Dabei benutzen wir die in § 290, Bd. I gegebene Lösungsmethode. Wir setzen, indem wir in der allgemeinen Gleichung vierten Grades das Glied mit z^3 getilgt denken, was ja durch einfache lineare Transformation bewirkt werden kann,

$$z^4 - 12az^2 - 16bz + 12c = (z^2 + 2v_2z + q)(z^2 - 2v_2z + q_1) = 0.$$

Um diese Zerlegung hervorzubringen, muss

$$q_1 = 2v_2^2 - \frac{4b}{v_2} - 6a, \quad q = 2v_2^2 + \frac{4b}{v_2} - 6a;$$

$$(27) \qquad v_2^6 - 6av_2^4 + (9a^2 - 3c)v_2^2 - 4b^2 = 0$$

sein. Danach ergiebt sich v_2 durch die Kette

$$v_4^2 = (-a^3 + 3ac + 2b^2)^2 - (a^2 + c)^3,$$
$$v_3^3 = (-a^3 + 3ac + 2b^2) + v_4,$$
$$v_2^2 = 2a + v_3 + \frac{-a^3 + 3ac + 2b^2 - v_4}{(a^2 + c)^2} v_3^2.$$

Hieraus erhält man die Wurzeln der biquadratischen Gleichung, wenn man

$$v_1^2 = 6a + \frac{4b}{v_2} - v_2^2$$

setzt, in der einfachen Form

$$z_1 = v_2 + v_1.$$

Gehen wir von ihr aus und bilden wir zunächst die Norm nach v_1, so folgt

$$(z - v_2 - v_1)(z - v_2 + v_1) = z^2 - 2v_2 z + 2v_2^2 - 6a - \frac{4b}{v_2}.$$

Hier fällt also kein weiteres Radical fort. Bilden wir jedoch weiter die Norm nach v_2

$$\left(z^2 - 2v_2 z + 2v_2^2 - 6a - \frac{4b}{v_2}\right)\left(z^2 + 2v_2 z + 2v_2^2 - 6a + \frac{4b}{v_2}\right)$$
$$= (z^2 + 2v_2^2 - 6a)^2 - \left(2v_2 z + \frac{4b}{v_2}\right)^2$$
$$= z^4 - 12az^2 - 16bz + \left(4v_2^4 - 24av_2^2 + 36a^2 - \frac{16b^2}{v_2^2}\right),$$

so giebt die Benutzung von (27) das Resultat

$$= z^4 - 12az^2 - 16bz + 12c;$$

hier verschwindet also mit v_2 zugleich v_3 und v_4, trotzdem $p_2 = 2$ und $p_3 = 3$, $p_4 = 2$ war. Bei einem Endradical wäre eine solche Tilgung nicht möglich gewesen.

Zweiundsechzigste Vorlesung.

Die Auflösbarkeit algebraischer Gleichungen.

§ 602. Eine der interessantesten Fragen der Albgebra ist die, ob jede Gleichung „auflösbar“ ist. Nachdem es gelungen war, die Gleichungen zweiten, dritten und vierten Grades aufzulösen, d. h. die expliciten Ausdrücke für ihre Wurzeln lediglich mit Hülfe von Wurzelzeichen darzustellen, richteten sich die Bemühungen der Algebraiker darauf, das gleiche Problem für den fünften Grad zu erledigen. Alle

hierauf verwendeten Anstrengungen waren aber vergebens, und so wandelte sich das Problem allmählich in das andere um, zu entscheiden, ob die Gleichungen fünften Grades überhaupt in dieser Form lösbar seien; oder noch allgemeiner, welche Gleichungen fünften Grades lösbar seien. P. Ruffini war der Erste, welcher die Unmöglichkeit der Auflösung allgemeiner Gleichungen höherer Grade bestimmt behauptete und zu beweisen versuchte. Seine Verdienste sind von H. Burkhardt*) eingehend gewürdigt worden. Gauss scheint einen Beweis für die Unauflösbarkeit besessen zu haben**); Abel publicirte 1826 einen solchen und beschäftigte sich auch weiterhin eingehend mit diesen Fragen, über die eine von ihm selbst nicht veröffentlichte Abhandlung vorhanden ist***). An seine Untersuchungen schliesst sich eine vervollständigende und abkürzende Darstellung L. Kronecker's an†), die wir in unserer Auseinandersetzung theilweise benutzen.

§ 603. Die allgemeine Frage lautet in unserer jetzigen Sprechweise: Kann eine Wurzel z_1 jeder irreductiblen algebraischen Gleichung $f(z) = 0$ als Radicalgrösse dargestellt werden?

Gesetzt es wäre eine solche Darstellung etwa für die Gleichung $f(z) = 0$ möglich, dann könnten wir unter Beibehaltung der Bezeichnungen unserer vorigen Vorlesung hinsichtlich der Ketten

$$z_1 = m_0 + v_1 + m_2 v_1^2 + m_3 v_1^3 + \cdots \tag{1}$$

setzen. Wenn wir von vornherein die Einheitswurzeln, soweit sie nothwendig sind, zum Rationalitätsbereiche ziehen, ist es erlaubt (§ 595) den Coefficienten von v_1^1 gleich 1 zu setzen, wie dies soeben geschehen ist.

Tragen wir (1) in $f(z) = 0$ ein, so entsteht, da alle Potenzen von z_1 in ähnliche Form gebracht werden können, die Identität

$$f(z_1) = M_0 + M_1 v_1 + M_2 v_1^2 + \cdots + M_{p_1-1} v_1^{p_1-1} = 0.$$

Nach dem Abel'schen Hülfssatze (A) in § 594 folgt daraus, dass $M_0, M_1, M_2, \cdots$ einzeln verschwinden; setzt man also

$$z_{\lambda+1} = m_0 + v_1 \omega_1^{\lambda} + m_2 v_1^2 \omega_1^{2\lambda} + m_3 v_1^3 \omega_1^{3\lambda} + \cdots \tag{2}$$
$$(\lambda = 0, 1, \cdots p_1 - 1)$$

*) Die Anfänge der Gruppentheorie und Paolo Ruffini, Abhandl. z. Geschichte d. Mathematik VI; Supplement zur Zeitschr. f. Math. u. Phys. v. Schlömilch (1892).

**) Demonstr. nova etc. Werke III, p. 17, Nr. 9: „Forsan non ita difficile foret, impossibilitatem iam pro quinto gradu omni rigore demonstrare, de qua re alio loco disquisitiones meas fusius proponam."

***) Werke, édit. Sylow et Lie, II, p. 217.

†) Berl. Ber. 1879, 3. März, p. 205.

und bedenkt, dass dann entsprechend

$$f(z_{\lambda+1}) = M_0 + M_1 v_1 \omega_1^{\lambda} + M_2 v_1^2 \omega_1^{2\lambda} + \cdots + M_{p_1-1} v_1^{p_1-1} \omega_1^{(p_1-1)\lambda}$$

wird, so ergiebt sich, dass $z_2, z_3, \cdots z_{p_1}$ gleichfalls Wurzeln von $f(z)=0$ sind. Dass diese sämmtlich von einander und von z_1 verschieden sind, zeigt wieder der auf die Differenz von zweien unter ihnen angewendete Satz (A). Demnach ist das Product

$$(z-z_1)(z-z_2)\cdots(z-z_{p_1})$$

oder die Norm

$$N(z-z_1), \quad \text{im Gebiete} \quad (v_2, \cdots v_\nu; \mathfrak{R})$$

genommen, ein Theiler von $f(z)$. Diese Norm ist sicher von v_1 frei; möglicherweise verschwinden in ihr noch die Radicale $v_2, v_3, \cdots v_{a-1}$, während v_a wirklich auftritt. Wir setzen, um das Auftreten des v_a durch die Bezeichnuug kenntlich zu machen,

$$(3) \qquad N(z-z_1) = (z-z_1)\cdots(z-z_{p_1}) = f_a(z;\, v_a, v_{a+1}, \cdots).$$

Im Gebiete $(v_a, v_{a+1}, \cdots v_\nu; \mathfrak{R})$ ist diese Function irreductibel. Als Norm von $z-z_1$ wird sie die Potenz einer irreductiblen Function in $(v_2, \cdots v_\nu; \mathfrak{R})$; da alle $z_1, z_2, \cdots$ von einander verschieden sind, muss es die erste Potenz sein; und die Irreductibilität gilt natürlich um so mehr für den engeren Rationalitätsbereich $(v_a, \cdots v_\nu; \mathfrak{R})$.

Wir bilden wieder die Norm von (3), also

$$Nf_a(z) \quad \text{im Gebiete} \quad (v_{a+1}, \cdots v_\nu; \mathfrak{R}),$$

nämlich das Product aus p_a Factoren

$$\prod_{\lambda} f_a(z;\, v_a\omega_a^{\lambda}, v_{a+1}, \cdots) \qquad (\lambda = 0, 1, 2, \cdots (p_a-1)).$$

Hierin ist sicher v_a verschwunden; möglicher Weise auch $v_{a+1}, \cdots$. Es sei v_b das erste darin wirklich vorhandene v; dann setzen wir, ähnlich wie oben, die Bezeichnung an

$$(4) \qquad Nf_a(z) = f_b(z;\, v_b, v_{b+1}, \cdots).$$

Wir weisen nun zunächst die Irreductibilität von f_b im Bereiche $(v_b, \cdots)$ nach. Ist $\varphi(z;\, v_b, \cdots)$ bei einer möglichen Zerlegung derjenige Factor von f_b, welcher $f_a(z;\, v_a, \cdots)$ enthält, dann kann man

$$(5) \qquad \begin{aligned} \varphi(z;\, v_b, \cdots) &= f_a(z;\, v_a, v_{a+1}, \cdots) \cdot \chi(z;\, v_a, v_{a+1}, \cdots) \\ &= q_0 + q_1 v_a + q_2 v_a^2 + \cdots \end{aligned}$$

setzen. Wegen (A) muss $q_1 = 0$, $q_2 = 0, \cdots$ sein; also ist auch bei Aenderung von v_a die Gleichung gültig

$$\begin{aligned} \varphi(z;\, v_b, \cdots) &= q_0 + q_1 v_a \omega_a^{\mu} + q_2 v_a^2 \omega_a^{2\mu} + \cdots \\ &= f_a(z;\, v_a\omega_a^{\mu}, v_{a+1}, \cdots) \cdot \chi(z;\, v_a\omega_a^{\mu}, v_{a+1}, \cdots). \end{aligned}$$

Es ist demgemäss φ durch jedes $f_a(z; v_a \omega_a^\mu, \cdots)$ bei $\mu = 0, 1, 2, \cdots p_a - 1$ theilbar. Da alle diese f_a in $(v_a, v_{a+1}, \cdots)$ irreductibel sind, so könnte nur dann φ nicht durch ihr Gesammtproduct theilbar sein, wenn zwei derselben einander gleich wären:

$$f_a(z; v_a \omega_a^\mu, v_{a+1}, \cdots) - f_a(z; v_a \omega_a^\nu, v_{a+1}, \cdots) = 0;$$

d. h. wenn man

$$f_a(z; v_a, v_{a+1}, \cdots) = r_0 + r_1 v_a + r_2 v_a^2 + \cdots; \qquad r_\lambda = (z; v_{a+1}, v_{a+2}, \cdots)$$

setzt, dann müsste die Gleichung gelten

$$r_1(\omega_a^\mu - \omega_a^\nu) + r_2 v_a(\omega_a^{2\mu} - \omega_a^{2\nu}) + \cdots = 0.$$

Aus (A) erkennt man, dass die Coefficienten aller Potenzen von v_a verschwinden müssen; weil nun nicht alle r gleich Null sein können, so folgt $\mu = \nu$.

Dies zeigt uns, dass der irreductible Factor φ mit f_b zusammenfällt, dass somit f_b selbst irreductibel im Gebiete $(v_b, \cdots v_\nu; \mathfrak{R})$ ist.

Wir haben ferner gesehen, dass $f(z)$ durch f_a theilbar ist; man kann demnach setzen:

$$\begin{aligned} f(z) &= f_a(z; v_a, v_{a+1}, \cdots) \cdot \psi(z; v_a, v_{a+1}, \cdots) \\ &= s_0 + s_1 v_a + s_2 v_a^2 + \cdots. \end{aligned}$$

Wendet man hier genau dieselbe Schlussweise an, wie sie bei (5) auseinandergesetzt wurde, so folgt, dass $f(z)$ durch alle conjugen Werthe von f_a theilbar ist, d. h. dass $f(z)$ die Function $f_b(z)$ als Factor enthält. Folglich sind auch alle im Gebiete $(v_b, v_{b+1}, \cdots v_\nu; \mathfrak{R})$ zu z_1 conjugen Werthe Wurzeln von $f(z) = 0$.

In derselben Weise kann man von $f_b(z)$ durch Normbildung weiter zu einem $f_c(z; v_c, \cdots)$ gehen, u. s. f., bis etwa auf $f_k(z; v_k, \cdots)$ ein $f_l(z) = f(z)$ folgt. Dann zeigt es sich, dass der Grad n von $f(z)$ gleich dem Producte

$$n = p_1 \cdot p_a \cdot p_b \cdots p_k \tag{6}$$

wird, und dass alle zu z_1 im Bereiche $(\mathfrak{R})$ conjuge Werthe Wurzeln von $f(z) = 0$ sind. Man kann also allen Grössen $v_\nu, v_{\nu-1}, \cdots v_2, v_1$ irgend welche mit den Definitionsgleichungen der v verträgliche Werthe geben, der Ausdruck (1) wird stets eine Wurzel von $f(z) = 0$ darstellen, aber nur $p_1 \cdot p_a \cdots p_k$ der erhaltenen Ausdrücke sind unter einander verschieden.

§ 604. Aus den Gleichungen (1) und (2) ergiebt sich durch Combination

$$(7) \qquad v_1 = \frac{1}{p_1}\left[z_1 + z_2\omega_1^{-1} + z_3\omega_1^{-2} + \cdots + z_{p_1}\omega_1^{-p_1+1}\right],$$

d. h. das letzte eingeführte Radical ist eine rationale, ganze Function von Wurzeln der Gleichung $f(z) = 0$ und von ω_1.

In (7) setzen wir an die Stelle von $z_1, z_2, \cdots z_{p_1}$ auf der rechten Seite beliebige Wurzeln, etwa $z_{i_1}, z_{i_2}, z_{i_3}, \cdots$ von $f(z) = 0$ und bezeichnen den so erhaltenen Werth der rechten Seite mit $v_{1,i}$. Nimmt man dann das Product

$$\prod_{(i)} \left(y - v_{1,i}^{p_1}\right) = g(y)$$

erstreckt über alle Wurzelpermutationen unter $z_1, z_2, \cdots z_n$, so ist $g(y)$ eine symmetrische Function der z und ihre Coefficienten finden sich also unter $(\omega_1; \mathfrak{R})$.

Es sei $g_1(y) = 0$ diejenige irreductible Gleichung in $(\omega_1; \mathfrak{R})$, bei der g_1 ein Theiler von g ist, und welche von dem Ausdrucke

$$(8) \qquad y_1 = v_1^{p_1} = n_0 + v_2 + n_2 v_2^2 + \cdots + n_{p_2-1} v_2^{p_2-1}$$

befriedigt wird, dann gilt von der Wurzel (8) von $g_1(y) = 0$ genau das Gleiche wie von der Wurzel z_1 von $f(z) = 0$, und daraus folgt, dass auch v_2 eine rationale, ganze Function der Wurzeln von $g_1(y) = 0$, also auch derjenigen von $f(z) = 0$ und von ω_1 und ω_2 wird.

Gehen wir so fort und beachten, dass wir jedes v in derselben Weise erlangen können, dann erhalten wir das Resultat: Jede der Radicalgrössen $v_\nu, v_{\nu-1}, \cdots v_2, v_1$, welche zur Darstellung der Wurzel einer auflösbaren irreductiblen Gleichung nöthig sind, ist eine ganze rationale Function von Wurzeln der Gleichung selbst und von Einheitswurzeln.

Schon in § 282 (Bd. I) haben wir diese Eigenschaft für die Gleichungen zweiten Grades

$$z^2 - 2a_1 z + a_2 = 0,$$

mit den Wurzeln

$$z = a_1 \pm \sqrt{a_1^2 - a_2}$$
$$= \frac{z_1 + z_2}{2} \pm \frac{z_1 - z_2}{2}$$

und in § 288 (Bd. I) für die Gleichungen dritten Grades hervorgehoben. Bei diesen wird, wenn man

$$z^3 - pz^2 + qz - r = 0$$

ansetzt, die Lösung gegeben durch

$$z_1 = \frac{1}{3}\left(p + W^{\frac{1}{3}} + \frac{p^2-3q}{W^{\frac{1}{3}}}\right); \qquad (\omega_3^3 = 1);$$
$$W = P + \sqrt{Q};$$
$$z_2 = \frac{1}{3}\left(p + \omega_3 W^{\frac{1}{3}} + \omega_3^2 \frac{p^2-3q}{W^{\frac{1}{3}}}\right); \qquad P = \frac{1}{2}(2p^3 - 9pq + 27r),$$
$$z_3 = \frac{1}{3}\left(p + \omega_3^2 W^{\frac{1}{3}} + \omega_3 \frac{p^2-3q}{W^{\frac{1}{3}}}\right); \qquad Q = P^2 - (p^2-3q)^3.$$

Wir haben dort gezeigt, dass die beiden Radicale die Form annehmen

$$\sqrt{Q} = 3\sqrt{-3}\,(z_1 - z_2)(z_2 - z_3)(z_3 - z_1),$$
$$\sqrt[3]{W} = z_1 + \omega_3^2 z_2 + \omega_3 z_3.$$

Die Lagrange'sche Methode der Lösung der Gleichungen vierten Grades führt zu den entsprechenden Resultaten (§ 291; Bd. I). Wir haben für

$$z^4 - 4c_2 z^2 - 8c_3 z - 4c_3 = 0$$

$$z_1 = \frac{1}{4}(t_1 + t_2 + t_3) \quad , \quad z_2 = \frac{1}{4}(t_1 - t_2 - t_3) \quad ,$$
$$z_3 = \frac{1}{4}(-t_1 + t_2 + t_3), \quad z_4 = \frac{1}{4}(-t_1 - t_2 + t_3),$$

wobei $t_1, -t_1;\ t_2, -t_2;\ t_3, -t_3$ die sechs Wurzeln von

$$t^6 - 4^2 \cdot 2c_2 t^4 + 4^4 \cdot (c_2^2 + c_4) t^2 - 4^6 c_3^2 = 0$$

sind. Nach dem Ergebnisse über die Gleichungen dritten Grades sind alle bei der Darstellung von t_1^2, t_2^2, t_3^2 auftretenden Radicalgrössen rational in den sechs Grössen t_α, und diese selbst wegen

$$t_1 = z_1 + z_2 - z_3 - z_4, \quad t_4 = -t_1 = -z_1 - z_2 + z_3 + z_4,$$
$$t_2 = z_1 - z_2 + z_3 - z_4, \quad t_5 = -t_2 = -z_1 + z_2 - z_3 + z_4,$$
$$t_3 = z_1 - z_2 - z_3 + z_4, \quad t_6 = -t_3 = -z_1 + z_2 + z_3 - z_4$$

in den Wurzeln z_α. Also sind es alle in die Wurzeldarstellung eintretenden Radicale.

Das zuerst einzuführende Radical besitzt den Werth

$$3\sqrt{-3}\,(t_1^2 - t_2^2)(t_1^2 - t_3^2)(t_2^2 - t_3^2)$$
$$= 2^6 3\sqrt{-3}\,(z_1 - z_4)(z_2 - z_3)\cdot(z_1 - z_3)(z_2 - z_4)\cdot(z_1 - z_2)(z_3 - z_4)$$

und steht also in engster Verbindung mit der Discriminante der Gleichung*).

---

*) Jacobi (Werke 3, p. 269) hat diese Darstellungen für die Gleichungen 2ten, 3ten, 4ten Grades ausführlich hergeleitet.

§ 605. Ist v_ν in der Kette der Radicale das oberste, d. h. das zuerst eingeführte Glied, dann kann v_ν nicht selbst bekannt sein, weil es sonst eben keiner neuen Einführung bedurft hätte, nachdem die Einheitswurzeln dem Rationalitätsbereiche zugeordnet waren; dagegen ist $v_\nu^{p_\nu}$ bekannt. Demnach gehört die Grösse

$$v_\nu = \varphi_\nu(z_1, \cdots z_n; \; \omega_1, \cdots)$$

nicht zur Gruppe G der Gleichung $f(z) = 0$, während $\varphi_\nu^{p_\nu}$ zu G gehört. Es ist also φ_ν eine Function der z, welche p_ν-mal mehr Werthe besitzt, als ihre p_ν^{te} Potenz. Die Frage nach der Existenz solcher Functionen haben wir in § 544 und § 545 erledigt und haben gefunden, dass ein solches φ_ν nur besteht, wenn G einen autojugen Theiler der Ordnung $\frac{n}{p_\nu}$ besitzt; v_ν gehört dann zu ihm.

Ist durch die Einführung von φ_ν die Gruppe G auf den autojugen Theiler G_1 mit dem Compositionsfactor p_ν reducirt, so wird $v_{\nu-1}^{p_{\nu-1}}$ aus gleichen Gründen, wie sie soeben für $v_\nu^{p_\nu}$ galten, noch zu G_1 gehören, dagegen $v_{\nu-1}$ nicht mehr. Es muss also, wenn ein $v_{\nu-1}$ vorhanden ist, einen weiteren autojugen Theiler G_2 von G_1 geben, und zu ihm muss der Compositionsfactor $p_{\nu-1}$ gehören. In derselben Art geht es weiter.

Umgekehrt haben wir im § 545 gleichfalls nachgewiesen, dass die Existenz solcher autojugen Theiler das Mittel zur Construction passender $v_\nu, v_{\nu-1}, \cdots$ in der Form

$$\varphi_\nu(z_1, \cdots z_n; \; \omega_1, \cdots), \quad \varphi_{\nu-1}(z_1, \cdots z_n; \; \omega_1, \cdots), \cdots$$

an die Hand giebt.

Wir haben demnach das Resultat: Es ist für eine auflösbare Gleichung charakteristisch, dass die Factoren $p_\nu, p_{\nu-1}, \cdots$ ihrer Compositionsreihe

$$(9) \qquad G, \; G_1, \; G_2, \; \cdots \; G_{\nu-1}, \; G_\nu = 1$$

sämmtlich Primzahlen sind. Die Ordnung der Gruppe G ist $(p_1 p_2 \cdots p_\nu)$; die Ordnung von $G_\varkappa$ ist gleich $(p_1 p_2 \cdots p_{\nu-\varkappa})$.

Gruppen, deren Compositionsfactoren ausschliesslich Primzahlen sind, heissen metacyklische oder auch auflösbare Gruppen.

Nach den in § 555 und § 556 jedesmal am Schlusse durchgeführten Untersuchungen können wir die soeben abgeleitete Bedingung auch in die Form bringen: Es ist für eine auflösbare Gleichung charakteristisch, dass die Substitutionen jeder Gruppe G_α ihrer Compositionsreihe bis auf Substitutionen der folgenden Gruppe $G_{\alpha+1}$ mit einander vertauschbar sind.

Es ist für eine auflösbare Gleichung charakteristisch, dass die Substitutionen jeder Gruppe ihrer Hauptreihe bis auf Substitutionen der folgenden Gruppe mit einander vertauschbar sind.

Natürlich ist in diesen Sätzen keine Lösung des Problems enthalten, sondern nur eine Umgestaltung, eine Uebertragung auf die Gruppen- oder die Substitutionentheorie. Gleichwohl aber sind diese Theoreme von ausserordentlich grosser Bedeutung. Denn ganz abgesehen von dem wichtigen Resultate, welches wir im folgenden Paragraphen daraus ziehen werden, zeigen sie uns, dass die Gruppe der Gleichung von höchster Bedeutung für die algebraische Auflösung einer Gleichung ist, derart dass die Gradzahl dagegen zurücktritt, weil eben die Constitution der Gruppe enger mit der Natur der Gleichung verknüpft ist. Es können zwei Gleichungen verschiedener Grade dieselbe, oder genauer gesprochen, einstufig isomorphe Gruppen besitzen — wie wir noch in dieser Vorlesung an einem wichtigen Beispiele sehen werden —, dann wird ihre Auflösung in beiden Fällen durch dieselben Hülfsmittel zu erreichen sein.

§ 606. In dem Falle, dass wir es mit einer allgemeinen Gleichung $f(z) = 0$, d. h. mit einer solchen zu thun haben, deren Gruppe die symmetrische ist, ergeben sich auf Grund unserer früheren Resultate noch weitere Folgerungen aus unseren Lehrsätzen des vorigen Paragraphen.

Wir wissen (§ 544), dass die alternirende Gruppe der einzige autojuge Theiler der symmetrischen Gruppe ist, und dass die Quadratwurzel aus der Discriminante, abgesehen von symmetrischen Factoren, die einzige rationale Function der Gleichungswurzeln ist, von der eine Potenz, nämlich die zweite, symmetrisch wird. Es ist folglich $p_\nu = 2$, und, wenn D die Discriminante bedeutet, am einfachsten und dabei völlig ausreichend

$$v_\nu = \sqrt{D}$$

zu setzen.

Es müsste jetzt, um in der Kette weiter gehen zu können, eine weitere Function $v_{\nu-1} = \varphi_{\nu-1}(z_1, \cdots z_n)$ bestimmt werden, die selbst nicht zweiwerthig ist, von der aber eine Primzahlpotenz es wird. Nach § 543, § 544, § 546 giebt es, falls $n > 4$ ist, eine solche Function $\varphi_{\nu-1}$ nicht mehr, weil die alternirende Gruppe A von mehr als vier Elementen einfach ist. Da die Ordnung von A ferner eine zusammengesetzte Zahl, nämlich $\frac{1}{2} n!$ ist, so entspricht der Uebergang von A zu 1 auch nicht den Forderungen, und deshalb ist die Bedingung

des vorigen Paragraphen nicht erfüllt; d. h.: **Die allgemeinen Gleichungen von höherem als dem vierten Grade haben keine Radicalzahlen als Wurzeln und sind daher nicht algebraisch auflösbar.**

§ 607. Wir kehren zu dem allgemeinen Falle einer auflösbaren Gleichung $f(z) = 0$ zurück, deren Gruppe G sein mag. Die Compositionsreihe dieser Gruppe werde durch die aufeinanderfolgenden Gruppen

$$(9) \qquad G,\ G_1,\ G_2,\ \cdots\ G_{\nu-1},\ G_\nu = 1$$

gegeben, derart dass der Rationalitätsbereich $(\mathfrak{R})$ der Reihe nach durch die Adjungirung der zu $G_1, G_2, \cdots$ gehörigen Functionen

$$(9^a) \qquad v_\nu,\ v_{\nu-1},\ \cdots\ v_2,\ v_1$$

vergrössert wird. Es gehört also v_α zu der Gruppe $G_{\nu+1-\alpha}$ für jeden Index α.

Gehen wir nun von $(z - z_1)$ durch Normbildung der Reihe nach wie im § 603 zu $f_a(z;\ v_a,\ v_{a+1}, \cdots),\ f_b(z;\ v_b,\ v_{b+1}, \cdots), \cdots$, so kommen wir zu einem $f_k(z;\ v_k,\ v_{k+1}, \cdots)$, welches bei nochmaliger Normbildung alle $v_k,\ v_{k+1}, \cdots v_\nu$ verschwinden lässt, so dass $f_l(z) = \Pi f_k(z;\ v_k, \cdots)$ zu $f(z)$ selbst wird. Bei dieser Normbildung zeigt sich die Bedeutung des Umstandes, dass mehr als ein v gleichzeitig verschwinden kann.

In $G_\nu = 1$ ist der Factor $(z - z_1)$ rational bekannt. Das ist er aber in $G_{\nu-1}$ nicht mehr; hier wird erst die Function

$$(9^b) \qquad f_a(z;\ v_a,\ v_{a+1}, \cdots) = (z - z_1)(z - z_2)\cdots(z - z_{p_1})$$

rational darstellbar werden, d. h. die Substitutionen von $G_{\nu-1}$ ändern zwar z_1, aber nicht (9^b). Hier wird z_1 mit $z_2, \cdots z_{p_1}$ in transitive Verbindung gesetzt. Weil nun aber auch $v_2, v_3, \cdots v_{a-1}$ in Wegfall gekommen sind, so werden auch die Substitutionen von $G_{\nu-2}, G_{\nu-3}, \cdots G_{\nu-a+1}$ nur die $z_1, z_2, \cdots z_{p_1}$ transitiv unter einander vertauschen, denn f_a ist, wie wir gesehen haben, in dem Bereiche $(v_a, v_{a+1}, \cdots v_\nu;\ \mathfrak{R})$ irreductibel.

Wenn man dann weiter zu $G_{\nu-a}$ übergeht, dann treten entsprechende Verhältnisse auf. Da erst f_b in dem neuen Bereiche rational bekannt und zugleich irreductibel ist, so wird in

$$(9^b) \qquad f_b(z;\ v_b,\ v_{b+1}, \cdots) = (z - z_1)(z - z_2)\cdots(z - z_{p_1 p_a})$$

die Reihe $z_1, z_2, \cdots z_{p_1 p_a}$ transitiv mit einander verbunden werden. Jede der Gruppen $G_{\nu-a}, G_{\nu-a-1}, \cdots G_{\nu-b+1}$ verbindet diese transitiv unter einander. Man erkennt aber den Unterschied der Bereiche, die durch $G_{\nu-a}, G_{\nu-a+1}, \cdots$ bestimmt sind, darin, dass $f_b = 0$ andere und andere Affecte aufweist.

Gehen wir nun den umgekehrten Weg, dann zeigt sich Folgendes: Zunächst ist $f = f_i = 0$ gegeben und die zugehörige Gruppe ist G. Durch $v_\nu, v_{\nu-1}, \cdots v_{k+1}$ hindurch führt die Adjunction, ohne dass $f = 0$ reductibel würde. Die Gruppen $G_1, \cdots G_{\nu-k}$ bleiben in sämmtlichen Wurzeln $z_1, z_2, \cdots z_n$ transitiv. Bei der Adjunction von v_k findet eine Zerfällung von $f = 0$ statt; demnach verbindet $G_{\nu-k+1}$ nur einen Theil der Wurzeln, nämlich $\frac{n}{p_k}$ transitiv mit einander. Alle diese so verbundenen Wurzeln z werden dann auch weiter in den Gruppen $G_{\nu-k+1}, \cdots G_{\nu-i}$ transitiv mit einander verbunden bleiben. Ebensowenig findet eine weitere Zerfällung von f_i statt. Dagegen wird bei $G_{\nu-i+1}$ eine neue Zerlegung in engere Systeme der Intransivität eintreten, u. s. f. bis zum letzten Male beim Uebergange von $G_{\nu-1}$ zu $G_\nu = 1$ eine Zerfällung und zwar in lineare Factoren eintritt.

§ 608. In der Folge (9^b) haben wir von jedem Gliede den Uebergang zum folgenden so gemacht, dass wir die Norm hinsichtlich des ersten eintretenden v mit kleinstem Index vornahmen. Wir wollen jetzt nach der Norm eines Gliedes in dem durch die ursprüngliche Gruppe G bestimmten Gebiete fragen.

Es möge

$$f_d(z) = (z - z_1)(z - z_2) \cdots (z - z_\delta) \qquad (\delta = p_1 p_a \cdots p_c)$$

vorliegen. Derjenige höchste Theiler von G, welcher nur $z_1, z_2, \cdots z_\delta$ transitiv unter einander verbindet, sei D mit der Ordnung ϑ. Da nun die Ordnung von G $r = p_1 p_2 \cdots p_\nu$ ist, so hat für die Substitutionen von G die Function f_d genau $r : \vartheta$ Werthe

$$f_d(z),\ f_d^{(1)}(z),\ f_d^{(2)}(z),\ \cdots,$$

die einander im Gebiete G conjug sind.

Jede der conjugen Functionen besitzt δ Factoren $(z - z_\alpha)$; in der Norm treten also insgesammt $\frac{r\delta}{\vartheta}$ solche auf. Ferner ist die Norm eine vollständige Potenz, und da G transitiv in $z_1, z_2, \cdots z_n$ ist, so kommt jede der Wurzeldifferenzen $(z - z_\alpha)$ gleich oft vor. Also ist für das Gebiet G

$$Nf_d(z) = f(z)^{\frac{r\delta}{\vartheta n}}.$$

Ist in der Reihe der Gruppen (9) $G_{\nu+1-d}$ die letzte, welche f_d ungeändert lässt, dann ist D ein Vielfaches von $G_{\nu+1-d}$, und ihre Ordnung wird

$$\vartheta = q \cdot (p_1 p_2 \cdots p_{d-1}),$$

wobei q eine ganze positive Zahl bedeutet. Ferner hat man

$$r = p_1 p_2 \cdots p_\nu; \quad \delta = p_1 p_a \cdots p_c; \quad n = p_1 p_a \cdots p_c p_d \cdots p_k,$$

und folglich wird der Exponent der Norm

$$\frac{r\delta}{\vartheta n} = \frac{p_d p_{d+1} \cdots p_\nu}{q \cdot p_d p_e \cdots p_k}.$$

Von besonderem Interesse ist der Fall, dass dieser Exponent den Werth 1 annimmt. Dazu ist es nöthig, dass D ein autojuger Theiler von G wird.

Nehmen wir zunächst an, D sei eine solche Gruppe, und f_d gehe unter dem Einflusse einer Substitution σ von G in

$$f_d^{(1)}(z) = \left(z - z_1^{(1)}\right)\left(z - z_2^{(1)}\right) \cdots \left(z - z_\delta^{(1)}\right)$$

über; dann gehört diese Function zu $\sigma^{-1} D \sigma = D$, und wenn also ein $z_\alpha^{(1)}$ gleich z_1 sein sollte, dann fallen alle $z^{(1)}$ mit den $z_1, z_2, \cdots z_\delta$ zusammen; das widerspräche dem Umstande, dass $f_d^{(1)}$ conjug zu f_d ist. Folglich enthält $f_d^{(1)}$ nur andere Wurzeln. So erkennt man, dass Nf_d gleich $f(z)$ selbst ist. Zugleich erkennt man, dass G eine imprimitive Gruppe ist, und dass die in einem f_d vereinigten z je ein Imprimitivitätssystem bilden.

Wenn umgekehrt in der Norm der Factor $(z - z_1)$ nur ein einziges Mal vorkommt, dann ist D autojug in G, und G ist imprimitiv. Die letzte Eigenschaft zeigt sich sofort, falls man bedenkt, dass jede Substitution σ, welche auf z_1 eine Wurzel $z_1, z_2, \cdots z_\delta$ folgen lässt, nur diese unter einander vertauscht; und dass jedes σ, welches auf z_1 ein $z_1^{(1)}, z_2^{(1)}, \cdots z_\delta^{(1)}$ folgen lässt, alle Wurzeln $z_1, z_2, \cdots z_\delta$ in diese neuen überführt. Da nun D von 1 verschieden sein soll, so folgt daraus auch, dass G zusammengesetzt und D in G autojug ist nach § 575.

Tritt der besprochene Fall ein, dann gelten also die über imprimitive Gleichungen früher abgeleiteten Theoreme;

$$f_d(z), \; f_d^{(1)}(z), \; f_d^{(2)}(z), \cdots$$

sind die Wurzeln einer Gleichung

$$\varphi(u) = u^{\frac{n}{\delta}} - \Theta_1 u^{\frac{n}{\delta}-1} + \cdots \pm \Theta_{\frac{n}{\delta}} = 0,$$

deren Coefficienten rational bekannt sind, und $z_1, z_2, \cdots z_\delta$ sind die Wurzeln von

$$f_d(z) = (z - z_1) \cdots (z - z_\delta) = 0.$$

Wir wollen nun zeigen, dass dies stets dann eintritt, wenn die Gradzahl n der zu Grunde gelegten auflösbaren Gleichung $f(z) = 0$ durch mehrere von einander verschiedene Primzahlen theilbar ist, wenn also die Compositionsfactoren nicht sämmtlich gleich sind.

Wir verfolgen die Compositionsreihe von G

$$(9^*) \qquad G,\ G_1,\ \cdots\ G_{\nu-k-1},\ G_{\nu-k},\ \cdots$$

bis zum ersten Gliede $G_{\nu-k}$, welchem ein Factor von geringerem als dem n^{ten} Grade

$$f_k(z;\ v_k,\ v_{k+1},\cdots) = (z-z_1)\cdots(z-z_\varkappa) \qquad (\varkappa = p_1 p_2 \cdots p_i)$$

entspricht, bei dem also zum ersten Male eine Zerfällung von $f(z)$ eintritt; es entstehen bei dieser p_k Factoren, da ja $n = \varkappa \cdot p_k$ ist.

Betrachten wir die Compositionsfactoren $p_\nu,\ p_{\nu-1},\ p_{\nu-2},\ \cdots$, so ist p_k der erste dieser Reihe, der in $n = p_1 p_a p_b \cdots$ auftritt. Nach der Annahme kommt unter $p_1,\ p_a,\ p_b,\ \cdots\ p_i$ noch ein von p_k verschiedener Compositionsfactor vor. Nach § 556 lässt sich demnach die Compositionsreihe in den auf $G_{\nu-k}$ folgenden Gliedern so einrichten, dass eine Gruppe G_σ in ihr auftritt, welche der Hauptreihe angehört, d. h. welche autojug in G selbst wird.

Ferner ist G_σ eine Subgruppe von $G_{\nu-k}$; und da $G_{\nu-k}$ nur z_1, $z_2, \cdots z_\varkappa$ mit einander transitiv verbindet, aber keine weiteren z, da also $G_{\nu-k}$ intransitiv ist, so gilt dasselbe von G_σ.

G_σ ist mithin ein intransitiver autojuger Theiler von G, und daher wird G eine imprimitive Gruppe (§ 575).

Wir sind daher zu dem folgenden wichtigen, zuerst von Abel*) ohne Beweis ausgesprochenen Satze gelangt: Ist der Grad n einer auflösbaren Gleichung $f(z) = 0$ durch zwei von einander verschiedene Primzahlen theilbar, dann ist die Gleichung imprimitiv, d. h. ihre Lösung kann durch diejenige einer auflösbaren Gleichung

$$u^{\frac{n}{\delta}} - \Theta_1 \cdot u^{\frac{n}{\delta}-1} + \cdots \pm \Theta_{\frac{n}{\delta}} = 0$$

mit rationalen Coefficienten, und die einer anderen auflösbaren Gleichung

$$f_d(z;\ v_d,\ v_{d+1},\cdots) = z^\delta - D_1(u) z^{\delta-1} + \cdots \pm D_\delta(u) = 0$$

mit in u rationalen Coefficienten bewirkt werden.

*) Édit. Sylow et Lie 2, p. 262.

Durch dieses Theorem ist die Frage nach den allgemeinen auflösbaren Gleichungen auf diejenige nach solchen auflösbaren Gleichungen reducirt, deren Grad die Potenz einer Primzahl ist. Denn wäre einer der Exponenten δ oder $\frac{n}{\delta}$ gleichfalls noch durch zwei von einander verschiedene Primzahlen theilbar, dann braucht man den Abel'schen Satz nur nochmals anzuwenden u. s. w.

Unsere ferneren Untersuchungen können sich also auf die auflösbaren Gleichungen mit Primzahlpotenzgrad beschränken.

§ 609. Im § 605 machten wir darauf aufmerksam, dass Gleichungen mit einstufig isomorphen Gruppen hinsichtlich ihrer Auflösbarkeit gleichen Charakter haben. Dies wollen wir an dem Verhalten der Gleichung verfolgen, welcher die Galois'sche Resolvente genügt.

Wir setzen, wie in § 560, mit unbestimmten Parametern u

$$\varpi_1 = u_1 z_1 + u_2 z_2 + \cdots + u_n z_n,$$

wenden hierauf alle Substitutionen s_i der Elemente z an, erlangen dadurch

$$\varpi_i = u_1 z_{i_1} + u_2 z_{i_2} + \cdots + u_n z_{i_n}$$

und bilden die Function

$$\gamma(\varpi) = (\varpi - \varpi_1)(\varpi - \varpi_2) \cdots (\varpi - \varpi_{n!}).$$

Im Rationalitätsbereiche von $f(z) = 0$ sei

$$g(\varpi) = (\varpi - \varpi_1)(\varpi - \varpi_2) \cdots (\varpi - \varpi_r)$$

ein irreductibler Factor von $\gamma(\varpi)$. Dann ist

$$g(\varpi) = 0$$

die zu $f(z) = 0$ gehörige Galois'sche Resolventengleichung, deren Gruppe nach § 577 gefunden werden kann. Wir bilden dem s_i entsprechend

$$\sigma_i = \begin{pmatrix} \varpi_1 & \varpi_2 & \cdots \\ \varpi_{i_1} & \varpi_{i_2} & \cdots \end{pmatrix}$$

für alle r Substitutionen der zu $f(z) = 0$ gehörigen Gruppe G. Die $\sigma_1, \sigma_2, \cdots \sigma_r$ bilden dann eine zu G einstufig isomorphe, der Gleichung $g(\varpi) = 0$ zugehörige Gruppe Γ. Die Compositionsfactoren für G und für Γ sind die gleichen; der Reihe und der Hauptreihe der Composition von G entsprechen die Reihe und die Hauptreihe der Composition von Γ.

Hat G nur Primzahlen als Compositionsfactoren, d. h. ist $f(z) = 0$ auflösbar, dann gilt dasselbe von $g(\varpi) = 0$. Der Grad von $g(\varpi)$ ist

$$r = p_1 \cdot p_2 \cdot p_3 \cdots p_\nu;$$

der Grad von $f(z)$ ist

$$n = p_1 p_a p_b \cdots p_k.$$

Macht man den Uebergang von G zu G_1, dann möge sich Γ auf Γ_1 reduciren. Γ_1 aber ist in $\varpi_1, \cdots \varpi_r$ intransitiv, auch wenn $f(z)$ bei G_1 noch irreductibel bleibt. Denn Γ_1 entsteht, wenn man die Substitutionen von G_1 auf $\varpi_1, \varpi_2, \cdots \varpi_r$ anwendet und deren dadurch bewirkte Umstellungen unter einander als Substitutionen σ deutet. Hierbei wird aber ϖ_1 durch G_1 nur in $\frac{r}{p_1}$ Werthe von ϖ_1 übergeführt werden können. Also muss Γ_1 die Elemente in p_1 Systeme von $\frac{r}{p_1}$ Wurzeln der Imprimitivität zerlegen.

So erkennt man allgemein, dass der Uebergang von Γ zu $\Gamma_1, \Gamma_2, \Gamma_3, \cdots$ jedesmal mit einer neuen engeren Zerfällung von $g(\varpi)$ verknüpft ist, bis beim letzten Schritte die einzelnen Factoren $\varpi - \varpi_1$, $\varpi - \varpi_2, \cdots$ selbst als rational heraustreten.

§ 610. Wir wollen zum Schlusse dieser Vorlesung die Voraussetzung fallen lassen, dass $f(z) = 0$ auflösbar sei, und wollen die Methode, die bisher auseinandergesetzt wurde, dazu verwenden, um die Lösung von $f(z) = 0$ auf ihre einfachsten Elemente zurückzuführen.

Die Gruppe von $f(z) = 0$ sei G; ferner sei G_1 ein autojuger Maximaltheiler von G. Unter $\varphi(z_1, \cdots z_n) = \varphi_1$ verstehen wir eine zu G_1 gehörige rationale Function von $z_1, z_2, \cdots z_n$; wendet man auf φ_1 die Substitutionen von G an, so entstehe

$$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_k; \tag{10}$$

es setzt dies voraus, dass die Ordnung der Gruppe G k-mal so gross ist, als die von G_1. Da G_1 autojug in G ist, so gehören $\varphi_1, \varphi_2, \cdots \varphi_k$ sämmtlich zu G_1, und jede dieser Functionen ist rational durch jede andere darstellbar.

Wir betrachten die Gleichung

$$\Phi(u) = (u - \varphi_1)(u - \varphi_2) \cdots (u - \varphi_k) = 0, \tag{11}$$

welche die Werthe (10) zu Wurzeln hat. Die Gruppe Γ von $\Phi(u)$ wird nach § 577 erhalten, wenn man auf (10) die Substitutionen von G anwendet und die Umstellungen als Substitutionen unter den φ deutet,

$$\sigma_i = \begin{pmatrix} \varphi_1 & \varphi_2 & \cdots & \varphi_k \\ \varphi_{i_1} & \varphi_{i_2} & \cdots & \varphi_{i_k} \end{pmatrix}.$$

Diese Gruppe Γ ist transitiv, und folglich ist (11) irreductibel. Weil ferner G_1 autojug in G ist, so wird nach § 559 die Gruppe Γ Factorgruppe von G und G_1, d. h.

$$\Gamma = G/G_1.$$

Endlich ist (11) eine einfache Gleichung, weil nach § 559 Γ nicht

mehr zusammengesetzt sein kann, da G_1 Maximalsubgruppe von G war, und nach § 575 muss (11) dann auch eine primitive Gleichung sein.

Durch die Auflösung von (11) und die Adjungirung aller oder auch nur einer ihrer Wurzeln wird somit $f(z) = 0$ auf eine Gleichung mit der Gruppe G_1 reducirt. Ist auch G_1 noch zusammengesetzt, dann können wir in gleicher Weise vorgehen und so die Auflösung auf diejenige einer Reihe von primitiven Gleichungen reduciren, deren Wurzeln in dem jedesmaligen Rationalitätsbereiche Galois'sche Resolventen sind. Die Grade der einzelnen Gleichungen sind als Compositionsfactoren invariant, d. h. dieselben, auf welchem Wege man auch die Auflösung liefern mag.

Dreiundsechzigste Vorlesung.

Auflösbare Gleichungen von Primzahlgrad.

§ 611. Ist eine Gleichung $f(z) = 0$ des Primzahlgrades p auflösbar, so sind ihre Wurzeln in der Form

$$
(1)\quad
\begin{aligned}
z_1 &= m_0 + v_1 + m_2 v_1^2 + \cdots + m_{p-1} v_1^{p-1},\\
z_2 &= m_0 + v_1\omega_p + m_2 v_1^2 \omega_p^2 + \cdots + m_{p-1} v_1^{p-1} \omega_p^{p-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
z_p &= m_0 + v_1\omega_p^{-1} + m_2 v_1^2 \omega_p^{-2} + \cdots + m_{p-1} v_1^{p-1} \omega_p^{-p+1}
\end{aligned}
$$

darstellbar, wobei ω_p eine primitive p^{te} Einheitswurzel bedeutet, und

$$
(2)\quad
\begin{aligned}
v_{\alpha-1}^{p_{\alpha-1}} &= F_{\alpha-1}(\mathfrak{R}),\\
v_{\alpha-2}^{p_{\alpha-2}} &= F_{\alpha-2}(v_{\alpha-1};\ \mathfrak{R}),\\
&\cdots\cdots\cdots\\
v_2^{p_2} &= F_2(v_3, \cdots v_{\alpha-1};\ \mathfrak{R}),\\
v_1^{p} &= F_1(v_2, \cdots v_{\alpha-1};\ \mathfrak{R})
\end{aligned}
$$

zu setzen ist. Gleich bei der ersten Normbildung, die an $(z - z_1)$ anknüpft,

$$
(3)\qquad f(z) = \prod (z - z_\alpha) \qquad (\alpha = 1, 2, \cdots p)
$$

fallen sämmtliche Kettenglieder $v_1, v_2, \cdots v_{\alpha-1}$ weg. Jede Aenderung der Bedeutung der v, die mit den Definitionsgleichungen (2) verträglich ist, wandelt daher v_1 in ein $m_\tau v_1^\tau \omega_1^{\varrho\tau}$ um [§ 598, (13) und § 600, (25)], und damit das System (1) in sich selbst. Jede mit der Constitution

der Gleichung verträgliche Umstellung der Wurzeln unter einander d. h. jede durch Substitutionen ihrer Gruppe hervorgerufene wird durch eine Aenderung in der Bedeutung der v bedingt. Daher werden die Substitutionen der zur Gleichung gehörigen Gruppe unter denen zu finden sein, die auf diesem Wege hergeleitet werden können.

Man erkennt dies auch auf folgende Weise. Es sei g in der Gleichung

$$g(z_1, z_2, \cdots z_p) = k \tag{4}$$

jede zur Gruppe G der Gleichung gehörige und daher rational bekannte Function $= k$. Dann gehört jede Aenderung unter den z_λ, welche diese Gleichheit (4) nicht stört, zu den Substitutionen der Gruppe G. Nun kann man (4) in die Form bringen

$$M_0 + M_1 v_1 + M_2 v_1^2 + \cdots + M_{p-1} v_1^{p-1} = k \tag{5}$$

und erkennt daraus, dass v_1 auch in $v_1 \omega_p^\alpha$ umgewandelt werden darf, dass also (4) die Substitution zulässt, die durch diese Aenderung hervorgerufen werden kann (§ 603).

Dieser Schluss gründet sich auf (A); zugleich wird dabei gezeigt, dass $M_1, M_2, \cdots M_{p-1} = 0$ sind, und $M_0 = k$ wird. Diese Gleichungen $M_\alpha =$ const. nehmen eine ähnliche Form wie (5) an, nur dass v_2 an die Stelle von v_1 tritt; und mithin folgt in gleicher Weise, dass auch die Bedeutung von v_2 beliebig geändert werden kann, so weit das mit (2) verträglich ist. So geht es weiter und daraus ist der ausgesprochene Satz ersichtlich.

§ 612. Wählen wir (4) wie oben so, dass g zur Gruppe gehört, nicht aber unter ihr steht, dann haben wir durch die letzte Beweisführung schon Substitutionen erlangt, die zu G gehören. Denn die Umwandlung von v_1 in $v_1 \omega_p$ führt z_1 in z_2, dieses gemäss (1) weiter in $z_3, \cdots$ und endlich z_p wieder in z_1 über. Es ist also

$$s = (z_1\ z_2\ z_3 \cdots z_p) \tag{6}$$

eine cyklische, zur Gruppe G von $f = 0$ gehörige Substitution. Mit ihr gehören natürlich auch alle Potenzen

$$s,\ s^2,\ s^3, \cdots s^{p-1},\ s^p = 1$$

zur Gruppe G. Hieraus ist schon ersichtlich, dass G transitiv ist, wie dies ja wegen der Irreductibilität von f sein musste.

Um weitere Substitutionen von G zu erhalten, betrachten wir die Umwandlung von v_1 in ein $m_\tau v_1^\tau \omega_p^{\varrho\tau}$ genauer. Gesetzt, es könnten bei irgend einer solchen Umwandlung zwei der Wurzeln, etwa z_α und z_β ungeändert bleiben, so müsste z_α in der Darstellung (1) das Glied

$(m_\tau v_1^\tau \omega_p^{\varrho\tau})\,\omega_p^{\alpha-1} = m_\tau v_1^\tau \omega_p^{\tau(\alpha-1)}$ enthalten, d. h. es wäre nothwendiger Weise

$$\omega_p^{\varrho\tau+\alpha-1} = \omega_p^{\tau(\alpha-1)} \tag{7}$$
$$\varrho\tau \equiv (\tau-1)(\alpha-1) \pmod{p}.$$

Ebenso würde sich wegen der Unveränderlichkeit von z_β ergeben, dass man zu gleicher Zeit auch hätte

$$\varrho\tau \equiv (\tau-1)(\beta-1) \pmod{p};$$

und da α von β verschieden ist, so würde aus den beiden letzten Gleichungen $\tau = 1$, $\varrho = 0$ folgen, d. h. zwei Wurzeln z_α und z_β können nur dann ungeändert bleiben, wenn v_1 in sich übergeführt wird. Dann bleiben aber alle Wurzeln z_λ an ihrer Stelle. G hat ausser der identischen Substitution 1 keine andere, die zwei der Wurzeln ungeändert lässt. (Vgl. § 572.)

Wenn nun eine Substitution von G nur eine Wurzel z_α ungeändert lässt, $z_{\alpha+1}$ dagegen in $z_{\alpha+\beta}$ umwandelt, dann gilt der ersten Annahme halber (7); und ferner muss wegen der zweiten Annahme

$$(m_\tau v_1^\tau \omega_p^{\varrho\tau})\,\omega_p^{\alpha} = m_\tau v_1^\tau \omega_p^{\tau(\alpha+\beta-1)}$$
$$\varrho\tau \equiv \tau(\alpha+\beta-1) - \alpha \pmod{p}$$

und folglich nach (7)

$$(\tau-1)(\alpha-1) \equiv \tau(\alpha+\beta-1) - \alpha \pmod{p}$$
$$\tau \equiv \frac{1}{\beta} \pmod{p}$$
$$\varrho \equiv -(\alpha-1)(\beta-1) \pmod{p}$$

sein. Es geht aber bei dieser Umänderung ein jedes z_γ in dasjenige z über, welches in der Darstellung (1) den Summanden

$$(m_\tau v_1^\tau \omega_p^{\varrho\tau})\,\omega_p^{\gamma-1} \quad \text{besitzt, der aus} \quad v_1\omega_p^{\gamma-1}$$

hervorgegangen ist. Setzt man den erhaltenen Werth von ϱ ein, so wird

$$\varrho\tau + \gamma - 1 \equiv \tau[-(\alpha-1)(\beta-1) + \beta(\gamma-1)] \equiv \tau[\alpha - 1 + \beta(\gamma-\alpha)];$$

folglich besitzt dasjenige z, in welches z_γ übergeht, den Summanden

$$m_\tau v_1^\tau \omega_p^{[\alpha-1+\beta(\gamma-\alpha)]\tau},$$

d. h. es ist $z_{\alpha(1-\beta)+\beta\gamma}$. Diejenige Substitution, welche z_α nicht ändert und $z_{\alpha+1}$ in $z_{\alpha+\beta}$ umwandelt, hat die Form

$$t_0 = |\, z_\gamma \quad z_{\alpha(1-\beta)+\beta\gamma} \,| \qquad (\beta \not\equiv 1). \tag{8}$$

Wenn endlich eine Substitution keins der z ungeändert lässt, dann darf bei festem ϱ und τ in $m_\tau v_1^\tau \omega_p^{\varrho\tau}$ kein α bestehen, welches (7)

befriedigt; denn sonst bliebe ja eben z_α unberührt. Dazu ist erforderlich und hinreichend, dass $\tau \equiv 1 \pmod{p}$ und ϱ nicht durch p theilbar ist. Hierdurch geht dann v_1 in $v_1\omega_p^\varrho$, also $v_1\omega_p$ in $v_1\omega_p^{\varrho+1}, \cdots$ über, d. h. z_1 in $z_{\varrho+1}$, ferner z_2 in z_ϱ u. s. f. Es giebt demnach nur die Substitutionen

$$(6) \qquad s = (z_1\ z_2 \cdots z_{p-1}\ z_p) = |\, z_\alpha \quad z_{\alpha+1} \,|$$

nebst deren Potenzen, welche sämmtliche z_α umstellen; (vgl. § 572).

Ausser der Einheit kann also G nur Substitutionen der Form (6) und (8) umfassen. G ist demnach mit der linearen Gruppe (§ 533) identisch, oder eine Subgruppe derselben. In unserem Falle von p Elementen haben wir es mit dem besonderen Falle der metacyklischen Gruppe zu thun (§ 534).

Die Form (8) lässt sich noch vereinfachen. Es ist nämlich

$$t_0 s^{\alpha(\beta-1)} = |\, z_\gamma \quad z_{\beta\gamma} \,|,$$

und umgekehrt lässt sich durch diese Substitution in Verbindung mit (6) wieder (8) herstellen. Wir können deswegen statt (8) nehmen

$$(8^a) \qquad t = |\, z_\gamma \quad z_{\beta\gamma} \,| \qquad (\gamma = 0, 1, 2, \cdots p-1).$$

Bedeutet nun e eine primitive Congruenzwurzel für den Modul p, so können wir $\beta = e^a$ setzen und statt (8^a) unter Weglassung des z

$$(8^b) \qquad t = |\, \gamma \quad e^a\gamma \,|$$

schreiben. Gesetzt es wäre in allen vorkommenden Substitutionen von der Form (8^b) die hingeschriebene diejenige, bei welcher der Exponent a von e den geringsten Werth annimmt, dann kommen unter den Substitutionen (8^b) nur solche

$$t^\varkappa = |\, \gamma \quad e^{\varkappa a}\gamma \,|$$

vor, bei denen der Exponent ein Vielfaches von a wird. Denn käme ein

$$\tau = |\, \gamma \quad e^b\gamma \,| \qquad (\sigma a < b < (\sigma+1)a)$$

vor, so folgte gegen die Annahme

$$\tau t^{-\sigma} = |\, \gamma \quad e^{b-\sigma a}\cdot\gamma \,| \qquad (0 < b - \sigma a < a).$$

Es sind somit alle Substitutionen von der Form (8^b) Potenzen einer unter ihnen. Diese Substitutionen sind die einzigen der Gruppe, welche z_0 ungeändert lassen. Wir wollen das a in (8^b) als den kleinstmöglichen Exponenten auffassen. Somit erkennen wir: Die Gruppe G einer auflösbaren Gleichung $f(z) = 0$ des Primzahlgrades p kann aus den beiden Substitutionen unter den z_u

$$(9) \qquad \begin{matrix} s = | u & u+1 | \\ t = | u & e^a u | \end{matrix} \quad (\text{mod.}\, p)$$

gebildet werden. Dabei bedeutet e eine primitive Congruenzwurzel für p. Ist k die niedrigste Zahl, für welche ak durch $(p-1)$ theilbar wird, so ist die Ordnung der Gruppe G gleich $p \cdot k$, also stets ein Theiler von $p(p-1)$. Für $k = p-1$ geht die Gruppe in die metacyklische über.

Ist r ein Theiler von $(p-1)$, so liefern die Substitutionen

$$(10) \qquad \begin{matrix} s = | u & u+1 | \\ t' = | u & e^{ar} u | \end{matrix} \quad (\text{mod.}\, p)$$

einen autojugen Theiler von (9).

Der letzte Satz folgt daraus, dass t' durch s und t transformirt bis auf Potenzen von s in sich übergeht. Man hat nämlich

$$s^{-1}t's = | u+1 \quad u | \cdot | u \quad e^{ar}u | \cdot | u \quad u+1 | = | u+1 \quad e^{ar}u+1 |$$
$$= | u \quad e^{ar}u + 1 - e^{ar} |;$$
$$t^{-1}t't = | e^a u \quad u | \cdot | u \quad e^{ar}u | \cdot | u \quad e^a u | = | e^a u \quad e^{ar+a} u | = | u \quad e^{ar} u |.$$

Wir können auch umgekehrt sagen, dass jede durch (9) gebildete Gruppe G die Gruppe einer auflösbaren Gleichung des Primzahlgrades p ist. Den Beweis stützen wir darauf, dass alle Compositionsfactoren für G Primzahlen werden. Ist nämlich k in seine Primfactoren zerlegt $= q_1 q_2 q_3 \cdots$, und betrachten wir zuerst die Gruppe G_1

$$(10^a) \qquad \begin{matrix} s = | u & u+1 |, \\ t_1 = | u & e^{aq_1} u | \end{matrix} \;,$$

so ist diese autojug in G mit dem Compositionsfactor q_1. Ferner betrachten wir die Gruppe G_2

$$(10^b) \qquad \begin{matrix} s = | u & u+1 |, \\ t_2 = | u & e^{aq_1q_2} u |, \end{matrix}$$

von welcher Aehnliches hinsichtlich G_1 gilt, u. s. f. So kommt man zu der Compositionsreihe $G, G_1, G_2, G_3, \cdots$, welche mit der aus den s^α gebildeten Gruppe K schliesst. Hierdurch ist die Behauptung erwiesen, da auch diese Gruppe K in der vorhergehenden autojug wegen

$$t^{-1}st = | e^{\varkappa a}u \quad u | \cdot | u \quad u+1 | \cdot | u \quad e^{\varkappa a}u | = | e^{\varkappa a}u \quad e^{\varkappa a}(u+1) |$$
$$= | u \quad u + e^{\varkappa a} | = s^{\varkappa a}$$

wird, und da alle Compositionsfactoren Primzahlen sind.

§ 613. Wir bilden eine zur arithmetischen Gruppe $K = [s^0, s, s^2, \cdots]$ gehörige, d. h. bei der Substitution $|u \quad u+1|$ unveränderliche Function $\varphi(z_1, z_2, \cdots)$; sie ist für die natürliche Folge der Indices cyklisch. Die Anzahl der Werthe, welche φ unter dem Einflusse von G annimmt, ist gleich k. Die durch G unter diesen Werthen hervorgerufenen Umstellungen bilden nach § 577 eine zu G isomorphe Gruppe Γ; und zwar ist Γ die Gruppe derjenigen Gleichung, von welcher die k Werthe φ_1, $\varphi_2, \cdots \varphi_k$ als Wurzeln abhängen.

Wir wollen nun nachweisen, dass Γ eine cyklische Gruppe wird, so dass also die $\varphi_1, \varphi_2, \cdots \varphi_k$ selbst Wurzeln einer cyklischen Gleichung sind.

Zu diesem Zwecke ordnen wir die Substitutionen von G in das Schema

$$\begin{array}{lllll} 1, & s\;, & s^2\;, & \cdots & s^{p-1} \\ t, & st\,, & s^2t\,, & \cdots & s^{p-1}t \\ t^2, & st^2, & s^2t^2, & \cdots & s^{p-1}t^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

ein; zu den einzelnen Zeilen gehören die Functionalwerthe

$$\varphi_1, \quad \varphi_2 = \varphi_t, \quad \varphi_3 = \varphi_{t^2}, \cdots \quad \varphi_k = \varphi_{t^{k-1}}.$$

Es fragt sich, was

$$\varphi_{s^\alpha t^\beta}, \; \varphi_{t s^\alpha t^\beta}, \; \varphi_{t^2 s^\alpha t^\beta}, \cdots \; \varphi_{t^{k-1} s^\alpha t^\beta} \tag{11}$$

werden wird. Nun ist, wenn wir $\gamma = \alpha e^{\alpha\beta}$ setzen,

$$s^\alpha t^\beta = |u \quad u+\alpha| \cdot |u \quad e^{\beta\alpha}u| = |u \quad e^{\beta\alpha}u + \alpha e^{\beta\alpha}| = t^\beta s^\gamma$$

und demnach

$$t s^\alpha t^\beta = t^{\beta+1} s^\gamma, \quad t^2 s^\alpha t^\beta = t^{\beta+2} s^\gamma, \; \cdots.$$

Folglich ist (11) identisch mit

$$\varphi_\beta, \; \varphi_{\beta+1}, \; \varphi_{\beta+2}, \cdots \; \varphi_{\beta-1};$$

und damit ist gezeigt, dass Γ eine cyklische Gruppe ist.

Löst man zuerst diese auf, dann reducirt sich G auf K. Daraus erkennt man: Die Auflösung jeder auflösbaren Gleichung von Primzahlgrad p wird durch die successive Lösung zweier cyklischen Gleichungen bewirkt, von denen die eine als Grad einen Theiler von $(p-1)$ oder $(p-1)$ selbst und die andere als Grad die Primzahl p hat.

Wir werden uns bald mit solchen Functionen $\varphi(z_1, z_2, \cdots z_p)$ genauer beschäftigen.

§ 614. Adjungiren wir einer auflösbaren irreductiblen Gleichung $f(z) = 0$ des Primzahlgrades p zwei beliebige ihrer Wurzeln, etwa z_α und z_β, dann wird durch diese Adjunction die Gruppe der Gleichung auf den Complex derjenigen unter ihren Substitutionen reducirt, welche z_α und z_β nicht ändern, d. h. auf 1.

Demnach ist nach dieser Adjunction jede beliebige Function rational bekannt; insbesondere gehört jedes z_γ dem Bereiche $(\mathfrak{R}; z_\alpha, z_\beta)$ an, d. h.: Man kann jede Wurzel z_γ als ganze rationale Function von z_α und z_β darstellen, mit Coefficienten, die dem gegebenen Rationalitätsbereiche $(\mathfrak{R})$ angehören

$$(12) \qquad z_k = g_k(z_\alpha, z_\beta) \qquad (k = 1, 2, \cdots p).$$

Wir wollen als Umkehrung zeigen: Wenn für alle Wurzeln z_1, $z_2, \cdots z_p$ einer irreductiblen Gleichung von Primzahlgrad die Beziehungen (12) für beliebige α, β herrschen, dann ist sie auflösbar. Gehen wir von der Voraussetzung dieses Satzes zu den für die Gruppe G der Gleichung daraus folgenden Eigenschaften über, so sehen wir erstens, dass G transitiv ist (§ 567); und zweitens, dass G ausser der Einheit keine Substitution besitzt, die z_α und z_β nicht umstellt; dabei sind α, β beliebige Elemente. Es besitzt also G ausser der Einheit keine Substitution, welche zwei Elemente nicht umstellt. Nach § 572 giebt es also nur $(p - 1)$ Substitutionen in G, die alle Elemente umsetzen, und diese Substitutionen werden cyklisch sein, da sonst passend gewählte Potenzen einige Elemente nicht ändern würden. Die Substitutionen, welche alle Elemente vertauschen, sind demnach Potenzen einer einzigen

$$s = (z_1 \; z_2 \; \cdots \; z_{p-1} \; z_p) = | \, u \quad u + 1 \, | .$$

Ausser diesen Potenzen giebt es nur noch Substitutionen von $(p - 1)$ Elementen. Es sei t eine solche, welche z_p nicht umsetzt. Dann muss $t^{-1} s t = s^\alpha$ werden, also muss t die Umstellung

$$\begin{pmatrix} z_1 & z_2 & z_3 & \cdots & z_p \\ z_\alpha & z_{2\alpha} & z_{3\alpha} & \cdots & z_p \end{pmatrix}$$

hervorrufen; d. h. man hat

$$t = (z_1 \; z_\alpha \; z_{\alpha^2} \cdots) \cdots = | \, u \quad \alpha u \, | .$$

Daraus folgt, dass die Gruppe der Gleichung die metacyklische ist oder unter der metacyklischen steht. Folglich ist die behauptete Umkehrung bewiesen: Wenn alle Wurzeln einer irreductiblen Gleichung von Primzahlgrad p sich durch zwei beliebige z_α, z_β rational darstellen lassen, ist sie auflösbar.

Aus dem zu Beginn des Paragraphen aufgestellten Satze folgt noch eine weitere Eigenschaft auflösbarer Gleichungen eines Primzahlgrades*). Enthält nämlich der Rationalitätsbereich ($\mathfrak{R}$) nur reelle Grössen, und sind zwei der Wurzeln von $f(z) = 0$, etwa z_α und z_β reell, dann zeigt (12), dass alle Wurzeln reell sind. **Eine auflösbare irreductible Gleichung des Primzahlgrades p hat entweder eine oder p reelle Wurzeln, wenn der Rationalitätsbereich nur reelle Grössen umfasst.** Wir finden dies bei den Gleichungen dritten Grades bestätigt. Von den Gleichungen fünften Grades können also solche irreductiblen, welche nur zwei complexe Wurzeln haben, nicht auflösbar sein.

§ 615. Wir gehen nun auf die Form (17) § 598 der Wurzeln einer auflösbaren Gleichung $f(z) = 0$ eines Primzahlgrades p zurück

$$
(13)\quad
\begin{aligned}
z_0 &= m_0 + R_0^{\frac{1}{p}} + R_1^{\frac{1}{p}} + \cdots + R_{p-2}^{\frac{1}{p}},\\
z_1 &= m_0 + R_0^{\frac{1}{p}}\omega + R_1^{\frac{1}{p}}\omega^e + \cdots + R_{p-2}^{\frac{1}{p}}\omega^{e^{p-2}},\\
z_2 &= m_0 + R_0^{\frac{1}{p}}\omega^2 + R_1^{\frac{1}{p}}\omega^{2e} + \cdots + R_{p-2}^{\frac{1}{p}}\omega^{2e^{p-2}},\\
&\cdots\cdots\cdots\cdots\cdots\cdots,
\end{aligned}
$$

wobei

$$
(14)\quad R_0^{\frac{1}{p}} = v_1, \quad R_1^{\frac{1}{p}} = m_e(R_0)\cdot v_1^e, \quad R_2^{\frac{1}{p}} = m_{ee}(R_0)\cdot v_1^{ee}, \quad \cdots
$$

gesetzt war. Aus (13) folgt

$$
(15)\quad
\begin{aligned}
R_0^{\frac{1}{p}} &= \frac{1}{p}[z_0 + z_1\omega^{-1} + z_2\omega^{-2} + \cdots],\\
R_1^{\frac{1}{p}} &= \frac{1}{p}[z_0 + z_1\omega^{-e} + z_2\omega^{-2e} + \cdots],\\
R_2^{\frac{1}{p}} &= \frac{1}{p}[z_0 + z_1\omega^{-e^2} + z_2\omega^{-2e^2} + \cdots],\\
&\cdots\cdots\cdots\cdots\cdots\cdots.
\end{aligned}
$$

Wenden wir auf $R_0, R_1, \cdots$ die cyklische Substitution $|u \ \ u+1|$ an, so bleiben diese Grössen ungeändert. Sie sind somit cyklisch für die Folge $z_0, z_1, z_2, \cdots z_{p-1}$.

---

*) L. Kronecker, Berl. Ber. 1856, 14. April, p. 204.

Wenden wir dagegen auf die Grössen (15) die Substitution

$$(16) \qquad | u \quad e^{-1}u |$$

an, so geht dabei jedes $R_\alpha^{\frac{1}{p}}$ in

$$\frac{1}{p}\left[z_0 + z_{e-1}\omega^{-e^\alpha} + z_{2e-1}\omega^{-2e^\alpha} + \cdots\right] = \frac{1}{p}\left[z_0 + \sum_k z_{ke-1}\omega^{-ke^\alpha}\right]$$

über. In der Summe können wir k durch he ersetzen, weil k und he gleichzeitig alle Reste mod. p durchlaufen; dann zeigt es sich, dass $R_\alpha^{\frac{1}{p}}$ in

$$\frac{1}{p}\left[z_0 + \sum_h z_h\omega^{-he^{\alpha+1}}\right] = R_{\alpha+1}^{\frac{1}{p}}$$

umgewandelt wird. Es ruft also (16) eine cyklische Verschiebung von

$$R_0^{\frac{1}{p}}, \ R_1^{\frac{1}{p}}, \ \cdots \ R_{p-2}^{\frac{1}{p}}$$

in der angegebenen Reihenfolge hervor.

Wir betrachten nun, indem wir einfach m statt m_e setzen, die Beziehung

$$R_1^{\frac{1}{p}} = m(R_0)\cdot R_0^{\frac{e}{p}}$$

und bemerken dabei, dass R_0 gemäss § 595 von Null verschieden ist. Die Substitution (16) liefert daraus

$$(17) \qquad \begin{aligned} R_2^{\frac{1}{p}} &= m(R_1)\cdot R_1^{\frac{e}{p}} \quad , \\ R_3^{\frac{1}{p}} &= m(R_2)\cdot R_2^{\frac{e}{p}} \quad , \\ &\cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \\ R_0^{\frac{1}{p}} &= m(R_{p-2})\cdot R_{p-2}^{\frac{e}{p}} ; \end{aligned}$$

und aus ihrer Combination entsteht, wie leicht zu sehen ist, die Gleichung

$$(17^a) \qquad R_0^{\frac{1-e^{p-1}}{p}} = m^{e^{p-2}}(R_0)\cdot m^{e^{p-3}}(R_1)\cdots m(R_{p-2}).$$

Wir wählen jetzt eine solche primitive Congruenzwurzel e, dass $(e^{p-1} - 1)$, welches stets durch p theilbar ist, keine höhere Potenz von p als Factor enthält. Das ist stets möglich; denn wenn jene

Differenz durch p^2 getheilt werden kann, wird $(p+e)^{p-1}-1$ sicher nicht p^2 enthalten, weil ja

$$(p+e)^{p-1}-e^{p-1}\equiv p(p-1)\cdot e^{p-2} \pmod{p^2}$$

wird. Wir setzen dann, indem wir den Factor p heraustreten lassen,

$$e^{p-1}-1=pq$$

und wählen t so, dass

$$\begin{aligned} qt+1 &\equiv 0 \pmod{p} \\ &= p\cdot r \end{aligned}$$

wird. Das ist erlaubt, weil q theilerfremd zu p ist. Danach wird

$$t\frac{1-e^{p-1}}{p}=-\frac{pqt}{p}=1-pr;$$

und setzen wir der Abkürzung halber

$$(18) \qquad et=t_1,\quad e^2t=t_2,\quad \cdots\quad e^{p-2}t=t_{p-2},$$

so entsteht aus (17ᵃ) durch Ausziehung der p^{ten} Wurzel, falls ω' eine p^{te} Einheitswurzel ist,

$$(17^b) \qquad R_0^{\frac{1}{p}}=\omega' R_0^r\cdot m^{\frac{t_{p-2}}{p}}(R_0)\cdot m^{\frac{t_{p-3}}{p}}(R_1)\cdots m^{\frac{t}{p}}(R_{p-2}).$$

Wir wollen zunächst nachweisen, dass die Grössen

$$(19) \qquad m^t(R_0),\ m^t(R_1),\ \cdots\ m^t(R_{p-2})$$

alle unter einander verschieden sind. Gesetzt, es wäre $m^t(R_a) = m^t(R_b)$, so zeigt (16), dass auch $m^t(R_{a+1})=m^t(R_{b+1})$ ist, u. s. f. Man schliesst nach bekannter Weise, dass es einen kleinsten Index α giebt, für welchen $m^t(R_\alpha)=m^t(R_0)$ wird, dass ferner α ein Theiler von $(p-1)$ ist, und dass endlich

$$\begin{aligned} m^t(R_0) &= m^t(R_\alpha) &&= m^t(R_{2\alpha}) &&= \cdots \\ m^t(R_1) &= m^t(R_{\alpha+1}) &&= m^t(R_{2\alpha+1}) &&= \cdots \\ &\cdots \end{aligned}$$

wird, wobei die Werthe in den verschiedenen Zeilen unter einander verschieden sind. Benutzt man dies für (17ᵇ), so tritt auf der rechten Seite zu $m^{\frac{t}{p}}(R_{p-2})$ der Exponent

$$\frac{1}{t}[t+t_\alpha+t_{2\alpha}+\cdots]=[1+e^\alpha+e^{2\alpha}+\cdots]=\frac{e^{p-1}-1}{e^\alpha-1}=\tau_0\cdot p;$$

ebenso zu $m^{\frac{t}{p}}(R_{p-3})$ der Exponent

$$\frac{1}{t}[t_1+t_{\alpha+1}+t_{2\alpha+1}+\cdots]=e[1+e^\alpha+e^{2\alpha}+\cdots]=e\frac{e^{p-1}-1}{e^{\alpha-1}}=\tau_1\cdot p,$$

u. s. w. Dabei sind $\tau_0, \tau_1, \tau_2, \cdots$ ganze Zahlen (Gauss, Disquisit. arithm. § 79).

Folglich entsteht an Stelle von (17^b) die Relation

$$R_0^{\frac{1}{p}} = \omega' R_0^r \cdot m^{\tau_0}(R_{\alpha-1}) \cdot m^{\tau_1}(R_{\alpha-2}) \cdots m^{\tau_{\alpha-1}}(R_0).$$

Ebenso erschliessen wir durch Anwendung von (16)

$$R_0^{\frac{1}{p}} = \omega' R_1^r \cdot m^{\tau_0}(R_0) \cdot m^{\tau_1}(R_{\alpha-1}) \cdots m^{\tau_{\alpha-1}}(R_1),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots .$$

Nach (13) und (14) wären also alle Wurzeln z_0 schon im Bereiche $(v_2, v_3, \cdots; \omega)$ rational darstellbar, was nach unseren Voraussetzungen über die Reductionen der Kette unmöglich ist (§ 594). Damit ist bewiesen, dass die Grössen (19) unter einander verschieden sind. —

Wir setzen nun

$$(19^a) \qquad m^t(R_0) = a_0, \quad m^t(R_1) = a_1, \quad \cdots \quad m^t(R_{p-2}) = a_{p-2},$$

dann sind dies Wurzeln einer cyklischen Gleichung des Grades $(p-1)$.

Denn $R_0, R_1, \cdots R_{p-2}$ sind es, weil ihre cyklischen Functionen für die aus

$$|u \quad u+1| \quad \text{und} \quad |u \quad eu|$$

entstehende Gruppe von $f(z) = 0$ unverändert bleiben und also bekannt sind (§ 527). Mit Hülfe des Theorems aus § 528 geht man dann zu (19^a) über.

Da die Grössen (19^a) von einander verschieden sind, so kann man auch R_0^r rational durch a_0, ebenso R_1^r rational durch a_1, u. s. w. in der Gestalt

$$R_0^r = \Phi(a_0), \quad R_1^r = \Phi(a_1), \quad \cdots$$

ausdrücken, wie das aus

$$(u-a_0)(u-a_1)\cdots\left[\frac{R_0^r}{u-a_0} + \frac{R_1^r}{u-a_1} + \cdots\right] = \psi(u)$$

in vielfach benutzter Schlussweise folgt. Zu dem Φ wollen wir den Factor ω' aus (17^b) ziehen.

Man hat somit

$$(20) \qquad \begin{aligned} R_0^{\frac{1}{p}} &= \Phi(a_0) \cdot \left(a_0^{\frac{e^{p-2}}{p}} \cdot a_1^{\frac{e^{p-3}}{p}} \cdots a_{p-3}^{\frac{e}{p}} \cdot a_{p-2}^{\frac{1}{p}}\right), \\ R_1^{\frac{1}{p}} &= \Phi(a_1) \cdot \left(a_1^{\frac{e^{p-2}}{p}} \cdot a_2^{\frac{e^{p-3}}{p}} \cdots a_{p-2}^{\frac{e}{p}} \cdot a_0^{\frac{1}{p}}\right), \\ &\cdots\cdots\cdots\cdots\cdots\cdots , \end{aligned}$$

wobei $a_0, a_1, a_2, \cdots a_{p-2}$ die Wurzeln einer cyklischen Gleichung des Grades $(p-1)$ bedeuten.

Dieser Uebergang von den R zu den a ist deswegen von Wichtigkeit, weil zwischen jenen gewisse Relationen (17) bestanden, während die a willkürlich sind. Denn wir werden nachweisen: Bedeuten umgekehrt die $a_0, a_1, \cdots$ die Wurzeln einer beliebigen cyklischen Gleichung $(p-1)^{\text{ten}}$ Grades, wobei die Ordnung $a_0, a_1, \cdots$ mit derjenigen der charakteristischen Substitution $(a_0 a_1 \cdots a_{p-2})$ der Gruppe der Gleichung übereinstimmt, und bildet man (20) und (13), so sind diese letzten Ausdrücke die Wurzeln einer auflösbaren Gleichung p^{ten} Grades mit rationalen Coefficienten.

Aus (20) ergiebt sich nämlich sofort die Richtigkeit der Relationen

$$R_1^{\frac{1}{p}} = \left(\frac{\Phi(a_1)}{\Phi(a_0)^e} a_0^{-q}\right) R_0^{\frac{e}{p}},$$

$$R_2^{\frac{1}{p}} = \left(\frac{\Phi(a_2)}{\Phi(a_1)^e} a_1^{-q}\right) R_1^{\frac{e}{p}},$$

$$\cdots\cdots\cdots,$$

woraus folgt, dass wenn $R_0^{\frac{1}{p}}$ vermöge anderer Deutung der p^{ten} Wurzeln in der ersten Formel aus (20) den Factor $\omega^{\varkappa}$ annimmt, dann $R_1^{\frac{1}{p}}$ den Factor $\omega^{e\varkappa}$ erhält, $R_2^{\frac{1}{p}}$ den Factor $\omega^{e^2\varkappa}$ u. s. w., so dass nur eine cyklische Vertauschung der Werthe (13) vor sich geht.

Ferner sind die einzigen unter den a_λ erlaubten Substitutionen die cyklische $s = (a_0 a_1 \cdots a_{p-2})$ und deren Potenzen. Wendet man $(a_0 a_1 \cdots a_{p-2})$ an, dann verschieben sich auch $R_0^{\frac{1}{p}}, R_1^{\frac{1}{p}}, \cdots R_{p-2}^{\frac{1}{p}}$ cyklisch, und dabei geht jedes z_α in $z_{\alpha e-1}$ über, d. h. man hat zwischen den z die Substitution

$$(16) \qquad |u \quad e^{-1}u|.$$

Demnach giebt es für die Grössen (13) nur die aus

$$|u \quad u+1| \quad \text{und} \quad |u \quad eu|$$

bestehende Gruppe. Damit ist der Satz bewiesen.

Die in (20) abgeleitete Form gab für die Gleichungen fünften Grades ohne Beweis Abel; die allgemeine Form hat, gleichfalls ohne

Beweis, Kronecker gegeben. Der erste vollständige Beweis stammt von H. Weber*). Diesem sind wir gefolgt.

Vierundsechzigste Vorlesung.

Auflösbare primitive Gleichungen von Primzahlpotenzgrad.

§ 616. Wir haben in § 608 gezeigt, dass es ausreicht statt allgemeiner auflösbarer Gleichungen solche zu behandeln, deren Grad eine Primzahlpotenz $p^{\varkappa}$ ist; aus denselben Ueberlegungen folgt, dass die Gleichung als primitiv vorausgesetzt werden kann, da anderenfalls eine weitere, früher gleichfalls behandelte Reduction des Problems vorgenommen werden kann.

Wir nehmen also an, $f(z) = 0$ wäre eine irreductible, primitive, auflösbare Gleichung des Grades $p^{\varkappa}$, wo p eine Primzahl bedeutet. Die Gruppe von $f(z) = 0$ sei G; G ist primitiv; und wir bezeichnen mit

$$(1) \qquad G, \; H, \; J, \cdots K, \; 1$$

die Hauptcompositionsreihe von G, so dass jede der Gruppen der höchste Theiler der vorhergehenden wird, der zugleich autojuger Theiler von G ist.

Keine der Gruppen von (1) ist intransitiv; denn nach § 575 ist eine zusammengesetzte Gruppe mit autojugem intransitiven Theiler selbst imprimitiv. Die Zerfällung von $f(z)$ in Factoren wird daher erst auf dem Uebergange von K zur Einheitsgruppe vor sich gehen. Zwischen K und 1 können sich Glieder der Compositionsreihe von G einschieben

$$(1^{a}) \qquad \cdots K, \; K^{(2)}, \; K^{(3)}, \cdots K^{(\lambda)}, \; 1;$$

alle diese gehören zu gleichen Compositionsfactoren, welche, da $f(z) = 0$ auflösbar ist, gleich der Primzahl p werden. Nach § 556 bildet die Gesammtheit der Substitutionen von K einen vertauschbaren Complex; d. h.: K ist eine Abel'sche Gruppe, deren p^{λ} Substitutionen durch

$$(2) \qquad s = \sigma_1^{\alpha} \sigma_2^{\beta} \sigma_3^{\gamma} \cdots \sigma_{\lambda}^{\varepsilon} \qquad (\alpha, \beta, \gamma, \cdots \varepsilon = 1, 2, \cdots p)$$

dargestellt werden können.

*) Abel, Brief an Crelle; Werke, éd. Sylow et Lie 2, p. 266. Kronecker, Berl. Ber. 1853, 10. Juni. Weber, Marburger Ber. 1892, p. 3; Algebra I, p. 638.

Wir bezeichnen nun eine der Wurzeln z mit $z_{0,0,\cdots 0}$, wobei λ Indices auftreten sollen, und diejenige Wurzel, in welche $z_{0,0,\cdots 0}$ durch (2) übergeführt wird, mit $z_{\alpha\beta\cdots\varepsilon}$. Gehört ferner

$$s_1 = \sigma_1^{\alpha_1}\sigma_2^{\beta_1}\sigma_3^{\gamma_1}\cdots\sigma_\lambda^{\varepsilon_1}$$

zu K, so wird diese Substitution $z_{00\cdots 0}$ in $z_{\alpha_1\beta_1\cdots\varepsilon_1}$ umwandeln und (ss_1) ruft

$$z_{\alpha+\alpha_1,\beta+\beta_1,\cdots\varepsilon+\varepsilon_1}$$

hervor. Daraus erkennt man, dass wir in analytischer Darstellung

(3) $$s \equiv | u_1, u_2, \cdots u_\lambda \quad u_1+\alpha, u_2+\beta, \cdots u_\lambda+\varepsilon | \pmod{p}$$

setzen können. Zugleich folgt, dass die Anzahl der Wurzeln

$$z_{\alpha\beta\cdots\varepsilon} \qquad (\alpha, \beta, \cdots \varepsilon = 1, 2, \cdots p)$$

gleich p^λ wird, d. h. dass p^λ der Grad der vorgelegten Gleichung, und also $\lambda = \varkappa$ sein muss. Ferner erkennt man, dass bei dem Uebergange in (1^a) von jeder der Gruppen K zur folgenden eine Zerfällung von $f(z)$ eintritt.

Aus (3) ersieht man, dass K gleich der arithmetischen Gruppe oder gleich einem ihrer Theiler ist. Bei einem Theiler aber würde einer der Indices nicht geändert werden, da ein Theiler nur dadurch entstehen kann, dass einer oder mehrere der Exponenten in (2) nicht von Null verschieden werden. Es fällt also K mit der arithmetischen Gruppe der Ordnung $p^\varkappa$ zusammen.

§ 617. Nun wissen wir aus § 553, dass die linearen Substitutionen die einzigen sind, welche die arithmetische Gruppe in sich selbst transformiren. Solche Substitutionen sind demnach gleichzeitig die einzigen, welche in G vorkommen können, da $G^{-1}KG = K$ sein muss. Das zeigt uns: Jede auflösbare primitive Gleichung des Grades $p^\varkappa$ hat eine Gruppe, welche in der linearen Gruppe

(4) $$| u_\varrho \quad a_{\varrho 1}u_1 + a_{\varrho 2}u_2 + \cdots + a_{\varrho\varkappa}u_\varkappa + d_\varrho | \qquad (\varrho = 1, 2, \cdots k)$$

des Grades $p^\varkappa$ enthalten ist.

Will man nun alle zu auflösbaren, primitiven, irreductiblen Gleichungen des Grades $p^\varkappa$ gehörigen Gruppen construiren, so kann der weitere Gang der Untersuchung der folgende sein. Bestimmt man die Grössen $\delta_1, \delta_2, \cdots \delta_\varkappa$ durch die Congruenzen (mod. p)

(5) $$a_{\varrho 1}\delta_1 + a_{\varrho 2}\delta_2 + \cdots + a_{\varrho\varkappa}\delta_\varkappa \equiv d_\varrho \qquad (\varrho = 1, 2, \cdots \varkappa),$$

so kann man (4) als Product

(6) $$| u_\varrho \quad a_{\varrho 1}u_1 + \cdots + a_{\varrho\varkappa}u_\varkappa | \cdot | u_\varrho \quad u_\varrho + \delta_\varrho | \qquad (\varrho = 1, 2, \cdots \varkappa)$$

darstellen; und diese Bestimmung ist stets möglich, weil für eine wirkliche Substitution (4) die Determinante der linken Seiten von (5) nicht durch p theilbar ist. Aus (6) ersieht man dann, dass man die Erweiterung der arithmetischen Gruppe nur durch homogene lineare Substitutionen zu bewirken braucht.

Es muss also zunächst zu K eine homogene lineare Substitution hinzugenommen werden, von der eine Primzahlpotenz $= 1$ wird. Dadurch entsteht in der Compositionsreihe, die wir von rechts her zu construiren haben, die vorletzte Gruppe. Damit muss wiederum eine Substitution verbunden werden, von der eine Primzahlpotenz in der eben erhaltenen vorletzten Gruppe vorkommt, u. s. w. so lange diese Operation fortgesetzt werden kann.

Das so fixirte Problem lässt sich aber sofort dadurch vereinfachen, dass wir die Betrachtungen auf die homogene lineare Gruppe beschränken.

Die Gruppe K der Substitutionen (3) ist nämlich autojug in G; wir können daher eine Factorgruppe G/K nach den Vorschriften des § 559 construiren. Wenn wir daselbst in der Formel (13) für die dortigen Substitutionen $1, s_2', s_3', \cdots$ unsere (3) nehmen, dann folgt, dass die dortigen s_2, s_3 durch die hier auftretenden homogenen Substitutionen von G ersetzt werden können, und dass die Composition der Elemente von G/K direct durch die Multiplication dieser homogenen Substitutionen ersetzt werden darf.

G/K kann demnach direct als Gruppe der in G enthaltenen homogenen Substitutionen aufgefasst werden. Somit hat diese Gruppe auch nur Primzahlen als Compositionsfactoren und ist also auflösbar.

Statt also G zu construiren, construiren wir die allgemeinste primitive, auflösbare, homogene Gruppe G/K und verbinden sie mit den Substitutionen (3) von K.

Wir wollen die dabei einzuhaltende Methode an dem Beispiele $\varkappa = 2$ darlegen, oder mit anderen Worten, wir wollen die allgemeinen Typen aller primitiven, auflösbaren Gleichungen der Ordnung p^2 feststellen, wo p eine Primzahl bedeutet*).

§ 618. Wir betrachten in der auflösbaren allgemeinen Gruppe G der

$$|\, h, k \quad a_1 h + b_1 k,\, a_2 h + b_2 k \,| \quad (\text{mod.}\, p)$$

die letzte Gruppe N der Hauptcompositionsreihe, welche nur unter einander vertauschbare Substitutionen enthält. Eine solche ist sicher vorhanden und von der Einheit verschieden (§ 556, Schluss). Sie ent-

*) C. Jordan, Journ. de math. (2) 13 (1868), p. 111.

hält, falls G allgemein, d. h. in keiner anderen von gleicher Eigenschaft enthalten ist, alle Substitutionen

(7) $$s_a = | h, k \quad ah, ak | \qquad (a = 0, 1, \cdots p-1).$$

Denn gehörte ein s_a nicht zu G, so könnte man, da die s_a mit jeder Substitution vertauschbar sind, eine solche Potenz s_a^ν von s_a bestimmen, dass eine Primzahlpotenz derselben zu G gehörte. Dann wäre auch $[G, s_a^\nu]$ auflösbar und allgemeiner als G, was den Annahmen widerspricht.

In N kommen demnach alle Substitutionen (7) vor. Wir betrachten zunächst den Fall, dass N ausser den s_a noch weitere Substitutionen enthält.

Es sei t eine weitere zu N gehörige Substitution. Wir können sie ohne Bedenken in der Normalform (§ 537) zu Grunde legen; denn durch die Transformation, welche eine beliebige Substitution in ihre Normalform überführt, werden die s_a immer nur wieder in sich selbst transformirt werden.

Je nach der Normalform haben wir verschiedene Fälle zu betrachten.

I) Es sei $t = | h, k \quad ah, bh + ak |$, wo $b \neq 0$ sein soll.

Ist nun eine willkürliche Substitution von N

$$\tau = | h, k \quad \mu h + \nu k, \mu_1 h + \nu_1 k |$$

und also

$$\tau^{-1} = \left| h, k \quad \frac{\nu_1 h - \nu k}{\mu\nu_1 - \mu_1\nu}, \frac{-\mu_1 h + \mu k}{\mu\nu_1 - \mu_1\nu} \right|,$$

so wird

$$\tau^{-1} t \tau = \left| h, k \quad \frac{[a(\mu\nu_1 - \mu_1\nu) - b\mu\nu]h - b\nu^2 k}{\mu\nu_1 - \mu_1\nu}, \frac{b\mu^2 h + [a(\mu\nu_1 - \mu_1\nu) + b\mu\nu]k}{\mu\nu_1 - \mu_1\nu} \right|.$$

Dies muss aber, weil t mit τ vertauschbar ist, wie dies aus der Annahme über N folgt, wieder $= t$ werden. Vergleicht man beide Formen, so ergiebt sich $\nu = 0$, und alle Substitutionen von N haben die Form

$$\tau = | h, k \quad \mu h, \mu_1 h + \mu k |.$$

Es sei ferner

$$\sigma = | h, k \quad mh + nk, m_1 h + n_1 k |$$

irgend eine Substitution der auflösbaren Gruppe G; dann muss $\sigma^{-1} t \sigma$ von der Form τ werden, da $G^{-1} N G = N$ ist. Vergleicht man in ähnlicher Weise wie soeben die beiden Formen, dann entsteht $n = 0$, und alle Substitutionen von G haben die Form

$$\sigma = | h, k \quad mh, m_1 h + mk |.$$

Diese Gruppe, mit den Substitutionen

$$| h, k \quad h + \alpha, k + \beta |$$

verbunden, giebt aber keine primitive Gruppe. Denn vereinigt man alle Wurzeln $z_{h,k}$ in ein System, welche das gleiche h haben, so erkennt man sofort, dass jede Substitution alle z mit gleichem h in andere z mit gleichem h umwandelt. Daher führt die Annahme eines solchen t auf keine brauchbaren Gruppen.

II) Es sei $t = |h, k \quad ah, bk|$, wobei a und b reelle Zahlen sind; $a \neq b$.

Ist nun eine willkürliche Substitution von N

$$\tau = | h, k \quad \mu h + \nu k, \mu_1 h + \nu_1 k |,$$

so wird $\tau^{-1} t \tau = t$. Vergleicht man beide Seiten, so ergiebt sich $\nu = 0$, $\mu_1 = 0$; jede Substitution von N wird

$$\tau = | h, k \quad \mu h, \nu_1 k |;$$

und da h und k reelle Indices sind, so werden auch μ und ν_1 reelle Zahlen.

Es sei ferner

$$\sigma = | h, k \quad mh + nk, m_1 h + n_1 k |$$

irgend eine Substitution der allgemeinen Gruppe G, dann muss $\sigma^{-1} t \sigma$ von der Form τ werden, da $G^{-1} N G = N$ ist. Daraus entnimmt man ebenso, dass entweder

$$n = 0, \quad m_1 = 0 \quad \text{oder} \quad m = 0, \quad n_1 = 0,$$

d. h. dass bei reellen Coefficienten $m_1, m; n_1, n$ unser σ entweder

$$(8) \qquad | h, k \quad mh, n_1 k | \quad \text{oder} \quad | h, k \quad nk, m_1 h |$$

ist. Hier können $m, n_1; n, m_1$ alle Zahlen $1, 2, \cdots p-1$ durchlaufen. Infolge dessen kann man die zweite Substitution durch

$$(9) \qquad | h, k \quad nk, m_1 h | \left| h, k \quad \frac{1}{m_1} h, \frac{1}{n} k \right| = | h, k \quad k, h |$$

ersetzen.

Dies giebt auch wirklich eine auflösbare Gruppe. Denn die $| h, k \quad mh, n_1 k |$ sind unter einander vertauschbar; und $| h, k \quad k, h |$ ist mit der durch jene gebildeten Gruppe vertauschbar:

$$| h, k \quad k, h |^{-1} \, | h, k \quad mh, n_1 k | \, | h, k \quad k, h | = | h, k \quad n_1 h, mk |.$$

Wir haben also einen ersten, aus

$$| h, k \quad h + \alpha, k + \beta |, \quad | h, k \quad mh, n_1 k |, \quad | h, k \quad k, h |$$

bestehenden Typus für G erlangt; α, β sind $= 0, 1, \cdots p-1$, und $m, n_1 = 1, 2, \cdots p-1$; die Ordnung von G beträgt somit $2(p-1)^2 p^2$. (Die Combinationen, bei denen m oder n_1 Null werden, mussten bei Seite bleiben, da ja die Determinante der Substitution nicht verschwinden durfte.)

III) Es sei endlich $t = | h, k \quad ah, bk |$, wobei a und b conjugirt complexe Zahlen

$$a = r + sj, \qquad b = r - sj;$$

und $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (j^2 = N)$

$$h = h_1 + k_1 j, \quad k = h_1 - k_1 j$$

bedeuten, und wobei N ein quadratischer Nichtrest für p ist (§ 537).

Es gelten alle unter II) durchgeführten Schlüsse, denen gemäss die Gruppe G/K aus allen

$$| h, k \quad ah, ak |, \quad | h, k \quad (r + sj)h, (r - sj)k |, \quad | h, k \quad k, h |$$

besteht. Bringen wir diese Substitutionen auf die reelle Form, so ergiebt sich

$$| h_1, k_1 \quad ah_1, ak_1 |, \quad | h_1, k_1 \quad rh_1 + sNk_1, sh_1 + rk_1 |, \quad | h_1, k_1 \quad h_1, -k_1 |,$$

wobei r, s beliebig gewählt werden können, falls nur die Determinante

$$(10) \qquad r^2 - s^2 N \not\equiv 0 \quad (\text{mod. } p)$$

ist. In dieser Form ist die erste Substitution gleichfalls enthalten, da $s \equiv 0$ gewählt werden kann; und (10) gestattet im Ganzen $(p^2 - 1)$ Lösungen.

Wir haben also einen zweiten, aus den Substitutionen

$$| h, k \quad h + \alpha, k + \beta |, \quad | h, k \quad rh + sNk, sh + rk |, \quad | h, k \quad h, -k |$$

bestehenden Typus für G erlangt; α, β sind $= 0, 1, \cdots p - 1$, und $r, s = 0, 1, \cdots p - 1$, falls nur die Combination $r = 0$, $s = 0$ ausgeschlossen wird. Dabei bedeutet N einen Nichtrest für den Modul p.

Die Ordnung von G beträgt daher $2(p^2 - 1)p^2$.

Hiermit ist der Fall erledigt, dass die höchste, aus unter einander vertauschbaren Substitutionen bestehende Gruppe der Hauptreihe von G eine höhere Ordnung besitzt als $(p - 1)p^2$.

§ 619. Wir betrachten jetzt den Fall, dass die Gruppe N ausser den

$$s_a = | h, k \quad ah, ak |$$

keine weiteren Substitutionen enthält.

Der Gruppe N möge in der Compositionsreihe als Gruppe höherer Ordnung die Gruppe M vorhergehen. Es sei t eine zu M gehörige Substitution. Wir können sie ohne Weiteres in der Normalform zu Grunde legen und unterscheiden nur je nach der Gestalt derselben wieder mehrere Fälle.

I) Es sei $t = | h, k \quad ah, bh + ak |$, wo $b \neq 0$ sein soll. Die Gruppe M entsteht aus der Verbindung von t mit den s_α. Alle Substitutionen von M haben die Form t, wenn man $b = 0$ zulässt. Bedeutet also

$$\sigma = | h, k \quad mh + nk, m_1 h + n_1 k |$$

irgend eine Substitution der gesuchten allgemeinen Gruppe G, dann muss, weil $\sigma^{-1} t \sigma$ entweder zu M selbst, oder doch zu einer dem M ähnlichen, in der vorhergehenden Gruppe der Hauptreihe enthaltenen M_1 gehört, diese Transformirte $\sigma^{-1} t \sigma$ von derselben Form wie t sein. Daraus folgt, wie in § 618 unter I), dass $n = 0$ und

$$\sigma = | h, k \quad mh, m_1 h + n_1 k |$$

wird. Dieselben Schlüsse wie dort zeigen uns dann, dass G imprimitiv ist. Diese erste Annahme ist also zu verwerfen.

II) Es sei $t = | h, k \quad ah, bk |$, wo entweder a und b reelle Zahlen sind, $a \neq b$; oder wo a und b zwei conjugirt complexe Zahlen $a = r + sj$, $b = r - sj$ bezeichnen.

Die Substitution t kann nicht für jede Substitution

$$\sigma = | h, k \quad mh + nk, m_1 h + n_1 k |$$

aus G der Gleichung $\sigma^{-1} t \sigma = t^\varkappa$ genügen; denn sonst würde t noch zu N gehören. Es giebt also ein von den $t^\varkappa$ verschiedenes

$$t_1 = \sigma^{-1} t \sigma = | h, k \quad \mu h + \nu k, \mu_1 h + \nu_1 k |,$$

welches mit den s vereinigt die Gruppe M_1 bilden möge, wobei $M \neq M_1$ ist, und M und M_1 der in der Hauptreihe von G nächsthöheren Gruppe L angehören. Aus diesem letzten Umstande folgt, dass t_1 und t bis auf eine Substitution s_f von N vertauschbar mit einander sind; d. h. man hat $t t_1 = t_1 t s_f$, oder ausführlicher geschrieben

$$\begin{aligned} &| h, k \quad a(\mu h + \nu k), b(\mu_1 h + \nu_1 k) | \\ = &| h, k \quad a\mu f h + b\nu f k, a\mu_1 f h + b\nu_1 f k |. \end{aligned}$$

Demgemäss müssen die vier Gleichungen erfüllt sein

$$a\mu = a\mu f, \quad a\nu = b\nu f; \quad b\mu_1 = a\mu_1 f, \quad b\nu_1 = b\nu_1 f.$$

Ist nicht gleichzeitig $\mu = 0$, $\nu_1 = 0$, dann folgt hieraus $f = 1$, $\mu_1 = 0$, $\nu = 0$; d. h.

$$t_1 = | h, k \quad \mu h, \nu_1 k |; \quad t t_1 = t_1 t.$$

Das kann aber nicht für alle aus t transformirten Substitutionen möglich sein, weil sonst die den $M, M_1, \cdots$ vorhergehende Gruppe L der Hauptreihe aus lauter vertauschbaren Substitutionen bestehen würde und demnach mit N zusammenfiele.

Es ist also gleichzeitig $\mu = 0$, $\nu_1 = 0$, und also $\mu_1 \nu \neq 0$. Dies ergiebt

$$a = bf, \quad b = af; \quad f^2 = 1.$$

Da ferner, wie soeben gezeigt worden ist, nicht beständig $f = 1$ sein kann, so wird

$$f = -1; \quad b = -a.$$

Es muss folglich sein

$$t = | h, k \quad ah, -ak |; \quad t_1 = | h, k \quad \nu k, \mu_1 h |.$$

Führt man hierin statt des Index h den durch

$$\eta = \frac{h}{\tau} \quad \text{mit} \quad \nu\tau^2 \equiv \mu_1 \quad (\text{mod.}\, p)$$

bestimmten Index η ein, so nehmen für $\nu\tau = \varrho$ die beiden Substitutionen einfachere Formen an. Wir können danach setzen

$$(11) \qquad t = | h, k \quad ah, -ak |, \quad t_1 = | h, k \quad \varrho k, \varrho h |.$$

Hieraus erhellt, dass t^2 wie t_1^2 zu N gehören. Folglich ist der Compositionsfactor beim Uebergange von M zu N gleich Zwei; $t^2 = s_{a^2}$, $t_1^2 = s_{\varrho^2}$.

Die Substitutionen (11), mit den s von N vereinigt, ergeben die Gruppe L der Hauptreihe, welche unmittelbar vor N steht. Denn jede Substitution von L muss t in ein ts_α und t_1 in ein $t_1 s_\beta$ transformiren. Stellt man die Bedingungen hierfür dar, dann zeigt sich, dass jede mögliche Substitution von L durch Multiplication einer Substitution (11) mit einem s aus N entsteht.

Demnach muss jede Substitution der allgemeinen Gruppe G die Substitutionen t, t_1 wieder in Substitutionen von L transformiren. Das giebt zunächst folgende neun Möglichkeiten. Eine beliebige Substitution v von G, die nicht zu L gehört, wandelt um

		1.	2.	3.	4.	5.	6.	7.	8.	9.
t	in	ts_α	ts_α	ts_α	tt_1s_α	tt_1s_α	tt_1s_α	t_1s_α	t_1s_α	t_1s_α.
t_1		ts_β	tt_1s_β	t_1s_β	ts_β	tt_1s_β	t_1s_β	ts_β	tt_1s_β	t_1s_β.

Von diesen Möglichkeiten fällt die dritte fort; denn bei ihr zeigt die wiederholt angewendete Methode der Formvergleichung, dass die transformirende Substitution zu L gehört.

Ferner fallen die 1[te], 5[te], 9[te] Möglichkeit fort, denn bei diesen würde $t \cdot t_1$ ein s als Transformirte ergeben, während doch ein s_μ nur in ein s_ν transformirt werden kann.

Ruft ferner die Transformation mit einem v_1 aus G die Umformung 4 hervor, so wird v_1^2 die Umformung 8 bewirken; und wenn ein v_0 umgekehrt 8 hervorbringt, so liefert v_0^2 wieder 4. Man kann sich also auf v_1 beschränken, und v_0 kann bei Seite gelassen werden.

Ruft endlich die Transformation mit einem v_2 aus G die Umformung 7 hervor, so wird $v_1 v_2$ und $v_1^2 v_2$ bezw. 6 und 2 bewirken.

Wir brauchen also nur v_1 und v_2 gemäss den Bestimmungen

$$(12)\qquad \begin{aligned} v_1^{-1} t v_1 &= t t_1 s_\alpha, \quad & v_1^{-1} t_1 v_1 &= t s_\beta; \\ v_2^{-1} t v_2 &= t s_\gamma, \quad & v_2^{-1} t_1 v_2 &= t t_1 s_\delta \end{aligned}$$

in allgemeinster Weise zu bestimmen, um G zu erhalten.

Setzt man

$$v_1 = | h, k \quad mh + nk, m_1 h + n_1 k |,$$

dann folgen aus (12) für die m, n; m_1, n_1 die acht Bedingungen

$$(13)\qquad \begin{aligned} m &= -\alpha\varrho n, \quad & n &= \alpha\varrho m\;; \quad & m_1 &= \alpha\varrho n_1, \quad & n_1 &= -\alpha\varrho m_1, \\ \varrho m_1 &= a\beta m, \quad & \varrho n_1 &= -a\beta n; \quad & \varrho m &= a\beta m_1, \quad & \varrho n &= -a\beta n_1. \end{aligned}$$

Zunächst zeigen diese Gleichungen, dass m, n; m_1, n_1 sämmtlich von Null verschieden sind. Die erste Zeile von (13) zeigt weiter, dass, wenn

$$j^2 \equiv -1 \pmod{p}$$

gesetzt wird, wobei wir nunmehr $p \equiv 1 \pmod{4}$ annehmen, um ein reelles j zu erhalten,

$$n = \pm jm, \quad n_1 = \pm jm_1$$

sein muss. Aus der zweiten Zeile entnimmt man

$$m_1 = \pm m, \quad n_1 = \pm n.$$

Durch Combination mit s_m kann man daher v_1 auf eine Form bringen, in welcher m durch 1 ersetzt wird; und ferner darf man wegen der Doppeldeutigkeit von j setzen $n = -j$ und also

$$v_1 = | h, k \quad h - jk, \pm(h + jk) |.$$

Weiter liefert (13) die Beziehungen

$$\alpha\varrho = -j, \quad \varrho = \pm a\beta,$$

und da man statt ϱ in (11) setzen kann $-\alpha\varrho$ und statt a ebenda $\mp a\alpha\beta$, so folgt an Stelle von (11), wenn man noch $\alpha = -1$, $\beta = 1$ setzt,

$$(11^a)\qquad \begin{aligned} t = | h, k \quad jh, -jk |, \quad t_1 = | h, k \quad jk, jh |; \\ v_1 = | h, k \quad h - jk, h + jk |. \end{aligned}$$

Dabei ist

$$v_1^2 = | h, k \quad (1-j)(h+k), (1+j)(h-k) |,$$
$$v_1^3 = | h, k \quad 2(1-j)h, 2(1-j)k |,$$

so dass v_1^3 zu N gehört.

Verfährt man genau so mit den Bedingungen der zweiten Zeile von (12), so findet man

$$v_2 = | h, k \quad h+k, h-k |, \tag{14}$$

so dass v_2^2 zu N gehört.

G setzt sich also, wenn $p \equiv 1 \pmod{4}$ ist, aus den Substitutionen

$$\begin{aligned}
&| h, k \quad h+\alpha, k+\beta |, && (\alpha, \beta = 0, 1, \cdots p-1);\\
&| h, k \quad ah, ak |, && (a = 1, 2, \cdots p-1);\\
&| h, k \quad jh, -jk |, && \\
&| h, k \quad jk, jh |, && j^2 \equiv -1 \pmod{p};\\
&| h, k \quad h-jk, h+jk |, && \\
&| h, k \quad h+k, h-k | &&
\end{aligned}$$

zusammen und besitzt daher die Ordnung $24(p-1)p^2$. Dies ist der dritte Typus.

Dass diese Gruppe wirklich den Bedingungen der Auflösbarkeit entspricht, ist leicht zu sehen.

Im Falle $p \equiv 3 \pmod{4}$ müssen wir, um eine reelle Form zu erhalten, anders verfahren. In diesem Falle ist -1 ein Nichtrest mod. p, und aus § 537, S. 292, Z. 10 folgt leicht, dass man

$$t = | h, k \quad \alpha h - \beta k, \beta h + \alpha k |$$

als Normalform nehmen kann. Ferner sei

$$t_1 = | h, k \quad \mu h + \nu k, \mu_1 h + \nu_1 k |$$

und wir suchen, unter welchen Bedingungen, wie oben, $tt_1 = t_1 t s_f$ wird. Man findet

$$\begin{aligned}
\alpha\mu - \beta\mu_1 &= \alpha\mu f + \beta\nu f, & \alpha\nu - \beta\nu_1 &= \alpha\nu f - \beta\mu f,\\
\alpha\mu_1 + \beta\mu &= \alpha\mu_1 f + \beta\nu_1 f, & \alpha\nu_1 + \beta\nu &= \alpha\nu_1 f - \beta\mu_1 f.
\end{aligned}$$

Bildet man die Determinante dieser vier in $\mu, \nu; \mu_1, \nu_1$ linearen Gleichungen, so folgt aus deren Verschwinden bei reellen Grössen $f = 1$, oder $f = -1$, $\alpha = 0$. Das Erste kann ebenso wenig stets vorkommen wie oben. Es muss also einmal der zweite Fall eintreten. Hier kann dann weiter durch Combination mit einem s_β

$$t = | h, k \quad -k, h |$$

angenommen werden; und daraus ergiebt sich als nothwendige Form

$$t_1 = | h, k \quad \mu h + \nu k, \nu h - \mu k |.$$

Nun ist $t^2 = | h, k \quad -h, -k |$ zu N gehörig; also muss das Gleiche mit t_1^2 stattfinden; dies ist auch in der That der Fall.

Die weiteren Entwickelungen verlaufen den oben gegebenen ganz analog; es reicht für die Construction von G aus, zwei Substitutionen v_1 und v_2 zu finden, welche den Bedingungen

$$v_1^{-1} t v_1 = t_1 t s_\alpha, \quad v_1^{-1} t_1 v_1 = t s_\beta;$$

bezw.

$$v_2^{-1} t v_2 = t_1 s_\gamma, \quad v_2^{-1} t_1 v_2 = t s_\delta$$

genügen. Setzt man, um zunächst die zweite dieser Substitutionen zu bestimmen,

$$v_2 = | h, k \quad mh + nk, m_1 h + n_1 k |,$$

so zeigt sich, dass die vier nöthigen Relationen, welche der ersten Forderung entsprechen,

$$-m_1 = (m\mu + n\nu)\alpha, \qquad -n_1 = (m\nu - n\nu)\alpha;$$
$$m = (m_1\mu + n_1\nu)\alpha, \qquad n = (m_1\nu - n_1\mu)\alpha$$

nur zu befriedigen sind, wenn

$$\alpha^2(\mu^2 + \nu^2) \equiv -1 \pmod{p}$$

wird. Das lässt sich für $p \equiv 3 \pmod{4}$ stets erfüllen. Sind μ_0, ν_0 Lösungen von

$$\mu_0^2 + \nu_0^2 \equiv -1 \pmod{p},$$

so kann man direct $\mu = \mu_0$, $\nu = \nu_0$, $\alpha = 1$ setzen. So kommt man auf das Resultat

$$t_1 = | h, k \quad \mu_0 h + \nu_0 k, \nu_0 h - \mu_0 k |,$$
$$v_2 = | h, k \quad \mu_0 h + (\nu_0 + 1)k, (\nu_0 - 1)h - \mu_0 k |.$$

Auf ähnliche Weise gelangt man zu

$$v_1 = | h, k \quad -(1 + \mu_0\nu_0)h + (\mu_0 - \nu_0^2)k, (\nu_0 + \mu_0^2)h + (\mu_0\nu_0 - \mu_0 + \nu_0)k |.$$

Es setzt sich also, wenn $p \equiv -1 \pmod{4}$ ist, G aus den Substitutionen

$$| h, k \quad h + \alpha, k + \beta |, \qquad (\alpha, \beta = 0, 1, \cdots p-1);$$
$$| h, k \quad ah, ak |, \qquad (a = 1, 2, \cdots p-1);$$
$$| h, k \quad -k, h |,$$
$$| h, k \quad \mu_0 h + \nu_0 k, \nu_0 h - \mu_0 k |, \qquad (\mu_0^2 + \nu_0^2 \equiv -1 \mod p);$$
$$| h, k \quad -(1 + \mu_0\nu_0)h + (\mu_0 - \nu_0^2)k, (\nu_0 + \mu_0^2)h + (\mu_0\nu_0 - \mu_0 + \nu_0)k |,$$
$$| h, k \quad \mu_0 h + (\nu_0 + 1)k, (\nu_0 - 1)h - \mu_0 k |$$

zusammen und besitzt daher die Ordnung $24(p-1)p^2$.

Es bliebe noch übrig, nachzuweisen, dass die abgeleiteten Typen nur primitive Gruppen ergeben, und Untersuchungen über ihre Allgemeinheit und Unabhängigkeit von einander anzustellen. Das wollen wir aber übergehen und verweisen nur auf die l. c. von C. Jordan in diesen Beziehungen aufgestellten Forschungen.

Erwähnt sei nur, dass für $p = 3$ der letzte Typus der einzige allgemeine ist.

§ 620. Zum Schlusse dieser Vorlesung wollen wir noch kurz auf die transitiven Gruppen von der Ordnung p^k, wobei p eine Primzahl bedeutet, eingehen. G sei eine solche Gruppe. —

Wir können den Begriff conjuger Substitutionen einer willkürlichen Gruppe M dem bisherigen Gebrauche dieses Ausdruckes entsprechend einführen. Ist σ_1 eine Substitution von M, so transformiren wir σ_1 durch alle Substitutionen von M und nennen die dabei als verschieden auftretenden $\sigma_2, \sigma_3, \cdots \sigma_\nu$ „zu σ_1 für die Gruppe M conjug". Eine Substitution ist „autojug", wenn bei diesen Transformationen stets das gleiche Resultat herauskommt, also $\nu = 1$ wird.

Die Einheit $\sigma_0 = 1$ ist in jeder Gruppe eine autojuge Substitution.

Alle autojugen Substitutionen in M bilden einen Theiler von M.

Die Anzahl ν aller zu σ_1 conjugen Substitutionen ist ein Theiler der Ordnung von M. Denn die μ Substitutionen von G, welche σ_1 in sich selbst transformiren, bilden einen Theiler H von M. Wenn dann $t_2^{-1}\sigma_1 t_2 = \sigma_2$ für die Substitution t_2 von M ergiebt, dann ist auch

$$(Ht_2)^{-1}\sigma_1(Ht_2) = \sigma_2;$$

die Substitutionen von Ht_2 sind die einzigen dieser Eigenschaft, und sie sind unter einander verschieden; ihre Anzahl beträgt also auch μ. So geht man weiter und erkennt, dass $\mu\nu$ gleich der Ordnung von M wird. Folglich ist ν ein Theiler der Ordnung von M. —

Wir wollen nun diese Begriffe für die Untersuchung unserer Gruppe G der Ordnung p^k verwenden. Wir fassen alle Substitutionen in Klassen zusammen, deren jede alle und nur die zu einer unter ihnen conjugen enthält. Die Anzahl der in jede Klasse eingehenden Substitutionen ist ein Theiler von $p^\varkappa$ und also eine Potenz von p. Die Klassen seien durch $s_0 = 1, s_1, s_2, \cdots$ charakterisirt, und die Zahlen der entsprechenden conjugen Substitutionen durch $p^{\alpha_0}, p^{\alpha_1}, p^{\alpha_2}, \cdots$ bezeichnet. Da $s_0 = 1$ autojug ist, so wird $p^{\alpha_0} = 1$. Fasst man nun alle Substitutionen zusammen, dann entsteht

$$p^k = p^{\alpha_0} + p^{\alpha_1} + p^{\alpha_2} + \cdots = 1 + p^{\alpha_1} + p^{\alpha_2} + \cdots.$$

Daraus ersehen wir, dass mindestens noch $(p-1)$ autojuge Substitutionen

in G vorhanden sind. Alle diese bilden einen Theiler von G; folglich ist ihre Anzahl eine Potenz von p, etwa p^{h_1} $(h_1 > 0)$.

Wir bezeichnen mit H_1 die Gruppe dieser p^{h_1} autojugen Substitutionen von G; H ist selbst autojug in G.

Die Factorgruppe

$$\Gamma_1 = G/H_1$$

hat die Ordnung p^{k-h_1}. Für Γ_1 gelten die eben angegebenen Schlüsse; Γ_1 hat einen autojugen Theiler H_1 der Ordnung p^{h_2}, in dem nur und alle autojugen Substitutionen von Γ_1 vorkommen. Dieser Gruppe H_1 ist in G eine Gruppe H_2 der Ordnung $p^{h_1+h_2}$ isomorph, deren Substitutionen, der Eigenschaft von H_1 entsprechend, unter einander bis auf Substitutionen von H_1 vertauschbar sind. Die Factorgruppe

$$\Gamma_2 = G/H_2$$

hat dann die Ordnung $p^{k-h_1-h_2}$; und alle früheren Schlüsse lassen sich auf sie wieder in Anwendung bringen.

So steigt man durch die Reihe von lauter zu G autojugen Gruppen

$$H_1, \; H_2, \; H_3, \; \cdots$$

bis G selbst auf. Jede von ihnen enthält nur Substitutionen, die mit einander bis auf diejenigen der vorhergehenden Gruppe vertauschbar sind. Daraus folgt, dass jede Gruppe einer Ordnung p^k eine auflösbare Gruppe ist; denn nach § 556, S. 337 kann man eine Compositionsreihe finden, die den Bedingungen aus § 605 entspricht.

Es möge noch angemerkt werden, dass der Grad einer irreductiblen Gleichung mit derartigen Gruppe gleichfalls eine Potenz von p ist.

Ist $p = 2$, dann liefern die betrachteten Gruppen alle diejenigen irreductiblen Gleichungen und nur diejenigen, deren Wurzeln geometrisch mit Hülfe von Zirkel und Lineal construirt werden können.

Fünfundsechzigste Vorlesung.

Der Casus irreducibilis. — Lösbarkeit im reellen Rationalitätsbereiche.

§ 621. Wir haben bei der Auflösung der cubischen Gleichungen darauf hingewiesen (§ 287; Bd. I), dass wenn bei der Gleichung dritten Grades mit reellen Coefficienten

$$(1) \qquad z^3 + 3c_2 z - 2c_3 = 0$$

die Discriminante $D = -108(c_2^3 + c_3^2)$ positiv ist, und also in dem Ausdrucke

$$z_\alpha = \omega^\alpha \sqrt[3]{c_3 + \sqrt{c_3^2 + c_2^3}} - \frac{\omega^{2\alpha} c_2}{\sqrt[3]{c_3 + \sqrt{c_3^2 + c_2^3}}} \qquad (\alpha = 0, 1, 2)$$

die innere Quadratwurzel imaginär wird, dass dann die drei Wurzeln z_0, z_1, z_2 gleichwohl reell werden; man hat also zur Erlangung dieser reellen Grössen scheinbar einen unnöthigen Weg durch das Complexe zu nehmen. Dieser Fall der Gleichungen dritten Grades heisst der „Casus irreducibilis“. Noch nicht entschieden ist aber bisher, ob dieser Weg nicht durch einen anderen, rein algebraischen ersetzt werden kann, der ganz im Gebiete reeller Rationalitätsbereiche verläuft und also die Verwendung jeder complexen Grösse vermeidet. Unter Benutzung goniometrischer Functionen gelingt dies ja.

Herr O. Hölder*) war einer der Ersten, die diese Frage erledigt und den Beweis dafür gegeben haben, dass ein solcher Weg nicht vorhanden ist. Wir wollen zunächst seinen Beweis reproduciren.

In § 587 ist Folgendes bewiesen worden: Es seien z_1 und y_1 die Wurzeln von zwei algebraischen Gleichungen

$$f(z) = 0 \quad \text{bezw.} \quad g(y) = 0, \tag{2}$$

deren Grade n und m sind; es werde ferner nach Adjunction von z_1 zu $g = 0$ die Grösse y_1 zur Wurzel einer irreductiblen Gleichung des Grades r, und nach Adjunction von y_1 zu $f = 0$ die Grösse z_1 zur Wurzel einer irreductiblen Gleichung des Grades s. Dann gilt die Proportion

$$n : m = s : r \qquad (r < m;\ s < n). \tag{3}$$

Hölder setzt nun weiter voraus, dass die Wurzeln der Gleichung $f = 0$ sämmtlich durch eine unter ihnen, etwa z_1, rational ausdrückbar seien; dann haben wir mit z_1 zugleich sämmtliche anderen Wurzeln $z_2, z_3, \cdots z_n$ von $f = 0$ der Gleichung $g = 0$ adjungirt. Es gilt demnach der Satz aus § 579, dass $g(y)$ nach dieser Adjungirung in irreductible Factoren gleichen Grades zerfällt wird. Folglich ist jetzt r ein Theiler von m.

Setzen wir ferner voraus, dass m eine Primzahl ist, so muss $r = 1$ werden; alle Factoren sind linear; jede der Wurzeln y_ν von $g(y) = 0$ ist rational im Bereiche $(\mathfrak{R}, z_1)$, wenn $\mathfrak{R}$ den ursprünglichen Rationalitätsbereich bedeutet. Sind demnach alle Elemente, die in $\mathfrak{R}$ eingehen, reell, und ist z_1 selbst reell, dann sind auch alle Wurzeln

*) Math. Ann. 38 (1891), p. 307.

von $g(y) = 0$ reell. Aus (3) folgt weiter auch, dass n ein Vielfaches von m ist.

§ 622. Nach diesen Vorbereitungen gehen wir von der cubischen Gleichung

$$(1) \qquad f(z) \equiv z^3 + 3c_2 z - 2c_3 = 0$$

aus und nehmen an, der vorgegebene Rationalitätsbereich $\mathfrak{R}$ sei reell. Es sei ferner $D = -108(c_2^3 + c_3^2)$ positiv, so dass die drei Wurzeln z_1, z_2, z_3 von $f = 0$ reell werden. Adjungiren wir nun $\sqrt{D}$, so wird

$$z_2 - z_3 = \frac{\sqrt{D}}{(z_1 - z_2)(z_1 - z_3)} = \frac{\sqrt{D} z_1}{2z_1^3 + 2c_3},$$

$$z_2 + z_3 = -z_1,$$

und es lassen sich deshalb alle Wurzeln z_α durch z_1 ausdrücken. Wir adjungiren nun, falls dies nöthig sein sollte, weitere Radicalgrössen, bis Alles zur Zerfällung von f vorbereitet ist; diese Radicalgrössen setzen wir gleichfalls als reell voraus. Die Zerfällung selbst möge endlich durch Adjunction einer reellen Wurzel der reinen Gleichung

$$g(y) \equiv y^m - a = 0$$

vor sich gehen, wobei m eine Primzahl ist, und a dem reellen Rationalitätsbereiche angehört. $g(y)$ ist irreductibel (§ 594); folglich stehen wir jetzt unter dem oben abgeleiteten allgemeinen Satze, und alle Wurzeln unseres $g = 0$ sind reell. Das geht nur, wenn $m = 2$ ist. Da aber gleichzeitig n ein Vielfaches von 2 sein müsste, während es hier gleich 3 war, so folgt die Unmöglichkeit der Auflösung des Casus irreducibilis im reellen Rationalitätsbereiche.

§ 623. Hölder verwendet die allgemeinen Resultate aus § 621 auch zur Ableitung weitergehender Sätze. Wir nehmen an, es soll $f(z) = 0$ eine irreductible Gleichung mit reellen Coefficienten sein, deren Wurzeln $z_1, z_2, \cdots$ sämmtlich als reell angenommen werden. Die Wurzel z_1 sei durch reelle Radicale darstellbar.

Um auch hier eine Gleichung zu gewinnen, deren Wurzeln sämmtlich durch eine unter ihnen ausdrückbar sind, gehen wir von $f(z)$ zur Galois'schen Resolventengleichung $F(\zeta) = 0$ über, wobei $\zeta_1 = u_1 z_1 + u_2 z_2 + \cdots$ ist. Auch $F = 0$ ist irreductibel, hat reelle Coefficienten und Wurzeln, und alle Wurzeln von $F = 0$ sind durch eine beliebige unter ihnen rational ausdrückbar.

Wenn nun durch Adjunction einer reellen Wurzel y_1 einer Gleichung

$$g(y) \equiv y^m - a = 0$$

des Primzahlgrades m zum ersten Male $f(z)$ in Factoren zerspalten wird, dann zerfällt dadurch auch $F(\zeta)=0$ in Factoren. Auf $F(\zeta)=0$ und $g(y)=0$ lässt sich dann der Satz von § 621 anwenden, und man erkennt, dass $m=2$ sein muss; ausserdem wird $r=1$, und $s=\frac{1}{2}n$. Die Galois'sche Gruppe von f reducirt sich also auf eine andere halb so hoher Ordnung, und zwar auf einen ihrer autojugen Theiler, da beide Wurzeln $\pm\sqrt{a}$ von $g(y)=0$ gleichzeitig adjungirt worden sind.

In dem neuen Bereiche $(\mathfrak{R}, \sqrt{a})$ gelten nochmals dieselben Voraussetzungen, und wir können dieselben Schlüsse ziehen. Dies kann so fortgesetzt werden, bis wir zu z_1 selbst gelangt sind. Diese Wurzel ist auf reellem Wege also nur zu erreichen, wenn sie durch eine Kette von Radicalgliedern des Grades 2 dargestellt werden kann. Nach § 620 ist also $f(z)$ selbst von einem Grade $2^\varkappa$. Nur dann kann eine Wurzel einer Gleichung $f(z)=0$ im Gebiete der reellen Grössen durch Radicale dargestellt werden, wenn die Gleichung als Grad eine Potenz von 2 hat und durch Quadratwurzeln lösbar ist.

§ 624. Auch der Kneser'sche Beweis*) geht von dem Satze (3) in § 621 aus. Dann aber benutzt er den Umstand, dass bei $n=3$ jede Zerfällung jedenfalls einen linearen Factor $(z-z_1)$ und daher $s=1$, $m=3r$ liefert. Ist nun m, wie angenommen wird, eine Primzahl >1, so folgt $m=3$, $r=1$, d. h. y_1 ist in $(\mathfrak{R}, z_1)$ rational.

Wir nehmen nun an, (1) sei im Gebiete der reellen Grössen durch Adjunctionen bis auf $(\mathfrak{R}')$ so weit vorbereitet, dass die weitere Adjunction einer reellen Wurzel von

$$g(y) \equiv y^m - A = 0$$

$f(z)$ zum Zerfallen bringt. Dann gelten die eben hergeleiteten Sätze, und es wird $m=3$ und

$$y_1 = \varphi(z_1; \mathfrak{R}'),$$

wo φ eine rationale Function in $(\mathfrak{R}')$ bedeutet. Aus dieser Gleichung folgt durch Substitution in die vorhergehende Gleichung

$$\varphi^3(z_1; \mathfrak{R}') = A.$$

Da aber z_1 die Wurzel der irreductiblen Gleichung $f(z)=0$ ist, so müssen auch die beiden Relationen

$$\varphi^3(z_2; \mathfrak{R}') = A, \quad \varphi^3(z_3; \mathfrak{R}') = A$$

bestehen. Die drei Grössen $\varphi(z_1; \mathfrak{R}')$, $\varphi(z_2; \mathfrak{R}')$, $\varphi(z_3; \mathfrak{R}')$ sind von

*) Math. Ann. 41 (1893), p. 344.

einander verschieden. Nach § 581 sind diese drei Werthe nämlich sämmtlich einander gleich oder sämmtlich von einander verschieden, und im ersten Falle wäre schon

$$y_1 = \varphi(z_1; \mathfrak{R}') = \frac{1}{3}[\varphi(z_1; \mathfrak{R}') + \varphi(z_2; \mathfrak{R}') + \varphi(z_3; \mathfrak{R}')]$$

ohne Adjunction von z_1, als symmetrische Function der Wurzeln von $f = 0$, rational bekannt.

Die Gleichung (1) möge jetzt drei reelle Wurzeln besitzen. Ferner sei $\mathfrak{R}'$ reell. Dann sind auch

$$\varphi(z_1; \mathfrak{R}'), \quad \varphi(z_2; \mathfrak{R}'), \quad \varphi(z_3; \mathfrak{R}') \tag{4}$$

reell. Es hätte also die Gleichung $u^3 = A$ die drei reellen Grössen (4) zu Wurzeln. Da dies nicht möglich ist, so war die Annahme, (1) könne im reellen Gebiete bis zur Zerfällung geführt werden, nicht statthaft. Damit ist wieder der behauptete Satz bewiesen.

§ 625. Eine andere Beweisführung stützt sich auf die Form der Wurzeln. Hier ist zunächst der Beweis von V. Mollame anzuführen, der erste, der von dem behandelten Theoreme gegeben worden ist*). Er zeigt, dass die Cardani'sche Wurzelform nicht zu vermeiden ist; und aus dieser Form folgt ja, wie wir früher gesehen haben (§ 285, Bd. I) die Richtigkeit des Satzes.

Einfacher baut sich auf denselben Principien ein Beweis von L. Gegenbauer auf**). Dieser geht davon aus, dass die Darstellung der Wurzeln einer auflösbaren Gleichung durch Radicale so beschaffen ist, dass der Exponent jedes Endradicals als Theiler des Grades der Gleichung auftreten muss.

Demnach hat die Wurzel z_1 jeder cubischen Gleichung die Form

$$z_1 = m_0 + m_1 v + m_2 v^2,$$

wobei v die Wurzel einer im Rationalitätsbereiche $(\mathfrak{R}')$ irreductiblen reinen Gleichung ist, und m_1, m_2 nicht gleichzeitig verschwinden können. Wie früher (§ 611) findet man für die anderen Wurzeln z

$$z_2 = m_0 + m_1 \omega v + m_2 \omega^2 v^2,$$
$$z_3 = m_0 + m_1 \omega^2 v + m_2 \omega v^2.$$

Aus diesen drei Gleichungen folgt durch Combination

*) Rend. d. R. Acc. d. Napoli (1890), 7. giugno. Daselbst finden sich auch einige historische Bemerkungen.

**) Monatshefte f. Math. 4 (1893), p. 155.

$$3m_0 = z_1 + z_2 + z_3,$$
$$3m_1 v = z_1 + \omega^2 z_2 + \omega z_3 = (z_1 - z_2) + \omega(z_3 - z_2),$$
$$3m_2 v^2 = z_1 + \omega z_2 + \omega^2 z_3 = (z_1 - z_3) + \omega(z_2 - z_3).$$

Wenn nun m_0, m_1, m_2, v und die drei Wurzeln z dem reellen Gebiete angehörten, dann müsste in den beiden letzten Gleichungen der Coefficient von ω gleich Null sein, d. h. $z_2 = z_3$. Das widerspräche aber der Voraussetzung der Irreductibilität unserer cubischen Gleichung.

Mit noch geringeren Voraussetzungen kommt Gegenbauer bei dem zweiten an gleicher Stelle gegebenen Beweise aus, den wir hier noch vereinfacht reproduciren.

Ist p ein bei der Darstellung einer Wurzel der irreductiblen Gleichung $f(z) = 0$ auftretender Exponent eines Endradicals, und zwar, wie gewöhnlich, eine Primzahl, so werden p Wurzeln der Gleichung durch Ausdrücke von der Form

$$z_{k+1} = m_0 + m_1 \omega_p^k v + m_2 \omega_p^{2k} v^2 + m_3 \omega_p^{3k} v^3 + \cdots \qquad (k = 0, 1, 2, \cdots)$$

gegeben, wobei $m_1, m_2, m_3, \cdots$ nicht gleichzeitig verschwinden können. Falls die Auflösung für z_1 im Gebiete der reellen Grössen vor sich geht, sind $m_0, m_1, m_2, \cdots$ und v reelle Grössen. Wenn weiter $f(z) = 0$ nur reelle Wurzeln hat, dann wird auch jede der Differenzen

$$z_{k+1} - z_{n-k+1} = 2i\left[m_1 \sin\frac{2k\pi}{p} \cdot v + m_2 \sin\frac{4k\pi}{p} \cdot v^2 + \cdots\right]$$

reell sein, und falls p von 2 verschieden ist, $z_{k+1} = z_{n-k+1}$. Das widerspricht der Irreductibilitätsvoraussetzung. Ist in einem reellen Rationalitätsbereiche eine irreductible Gleichung $f(z) = 0$ mit lauter reellen Wurzeln durch reelle Radicale lösbar, so sind alle in dem Ausdrucke einer Wurzel auftretenden Wurzelexponenten der Endradicale gleich 2. Eine derartige Gleichung ungeraden Grades existirt also nicht.

§ 626. In einer späteren Notiz leitet L. Gegenbauer*) allgemeinere Sätze mit Hülfe desjenigen einfachen Princips ab, welches beim Kneser'schen Beweise die entscheidende Rolle spielt (§ 624).

Es sei $f(z) = 0$ eine Gleichung in dem reellen Rationalitätsbereiche $(\mathfrak{R})$; $f(z) = 0$ soll keine in $(\mathfrak{R})$ rationale Wurzel besitzen. Weiter sei $g(y) = 0$ eine andere, irreductible Gleichung desselben Bereiches von einem Primzahlgrade mit den Wurzeln $y_1, y_2, \cdots y_m$.

*) Monatshefte f. Math. 6 (1895), p. 12.

Endlich soll es möglich sein, eine Wurzel z_1 rational in $(\mathfrak{R})$ durch eine Wurzel y_1 darzustellen in der Form

$$z_1 = \varphi(y_1; \mathfrak{R}).$$

Dann folgt, wie immer, dass jeder Functionswerth von φ

$$z_\lambda = \varphi(y_\lambda; \mathfrak{R}) \qquad (\lambda = 1, 2, \cdots m)$$

eine Wurzel von $f(z) = 0$ ist. Gesetzt, es wären zwei dieser Functionen φ einander gleich, etwa

$$\varphi(y_\alpha; \mathfrak{R}) = \varphi(y_\beta; \mathfrak{R}),$$

dann ergiebt sich nach vielfach angewendeter Schlussweise, dass alle Werthe $\varphi(y_\lambda; \mathfrak{R})$ einander gleich werden, weil m eine Primzahl bedeutet. Dadurch wird aber

$$z_1 = \varphi(y_1; \mathfrak{R}) = \frac{1}{m}[\varphi(y_1; \mathfrak{R}) + \varphi(y_2; \mathfrak{R}) + \cdots + \varphi(y_m; \mathfrak{R})]$$

als symmetrische Function der $y_1, y_2, \cdots y_m$ schon ohne Adjungirung von y_1 rational in $(\mathfrak{R})$, und daher müsste gegen die Annahme $f(z) = 0$ eine rationale Wurzel haben. Sonach sind alle p Werthe $\varphi(y_\lambda; \mathfrak{R})$ von einander verschieden und liefern deshalb auch p verschiedene Wurzeln von $f(z) = 0$. —

Bis hierher haben wir die Schlüsse schon im Kneser'schen Beweise verfolgt. Gegenbauer schliesst nun weiter: Hat $g(y) = 0$ also $\varkappa$ reelle Wurzeln, so sind alle entsprechenden $\varkappa$ Werthe $\varphi(y; \mathfrak{R})$ auch reelle Wurzeln von $f = 0$; d. h. die Gleichung $f(z) = 0$ besitzt mindestens so viele reelle Wurzeln wie $g(y) = 0$; oder mit anderen Worten: In einem reellen Rationalitätsbereiche ist die rationale Darstellung einer an sich nicht rationalen Wurzel z_1 durch eine Wurzel y_1 nur dann möglich, wenn $f(z) = 0$ mindestens so viele reelle Wurzeln besitzt, wie die irreductible Gleichung $g(y) = 0$ des Primzahlgrades m.

Ein ähnlicher Satz gilt von den complexen Wurzeln. Ist nämlich y_α complex und y'_α die zu y_α conjugirte Wurzel, so kann nicht $z_\alpha = \varphi(y_\alpha; \mathfrak{R})$ reell werden. Denn sonst wäre

$$\varphi(y'_\alpha; \mathfrak{R}) = \varphi(y_\alpha; \mathfrak{R}),$$

und so kämen wir wieder auf den oben als unstatthaft erkannten Fall. Es entsprechen demnach allen complexen Wurzeln von $g(y) = 0$ auch complexe, von einander verschiedene Wurzeln von $f(z) = 0$; d. h. die Gleichung $f(z) = 0$ besitzt mindestens so viele complexe Wurzeln wie $g(y) = 0$. Verbindet man diesen Satz mit dem ersten, soeben abgeleiteten, dann ergiebt sich das folgende Theorem: Ist $f(z) = 0$

eine Gleichung im reellen Gebiete $(\mathfrak{R})$, von der eine Wurzel z_1 rational darstellbar ist durch die Wurzel y_1 der in demselben Gebiete irreductiblen Gleichung $g(y) = 0$ eines Primzahlgrades, dann ist weder die Anzahl der reellen Wurzeln von $g(y) = 0$ noch diejenige der complexen Wurzeln grösser als die entsprechende Anzahl für $f(z) = 0$.

Nehmen wir nun $f(z) = 0$ als irreductibel an, dann ergiebt sich weiter, weil ja $f(z)$ durch die in $(\mathfrak{R})$ rationale Function

$$\prod_\lambda (z - \varphi(y_\lambda; \mathfrak{R})) \qquad (\lambda = 1, 2, \cdots m)$$

theilbar und also ihr gleich ist, dass erstens $n = m$ sein wird, zweitens dass jede Wurzel z_λ von $f(z) = 0$ durch eine Wurzel y_λ von $g(y) = 0$ rational darstellbar ist, und drittens dass z_λ und y_λ gleichzeitig reell und auch gleichzeitig complex sind. Wenn also insbesondere m ungerade, und

$$g(y) = y^m - A$$

ist, dann muss $f(z) = 0$ vom Grade m sein und darf nur eine einzige reelle Wurzel besitzen. Es ist nur dann möglich, eine reelle Wurzel z_1 einer irreductiblen Gleichung eines ungeraden Primzahlgrades im reellen Gebiete zu bestimmen, wenn diese Wurzel die einzige reelle der Gleichung ist.

Sechsundsechzigste Vorlesung.

Die Wendepunkte der Curven dritter Ordnung. Tripelgleichungen.

§ 627. Auf interessante auflösbare Gleichungen führt die Frage nach den Wendepunkten der Curven dritter Ordnung in der Ebene. Wir wollen hier alle nothwendigen Ableitungen zusammenstellen, auch die auf geometrische Verhältnisse sich beziehenden.

Dabei legen wir Dreieckscoordinaten x, y, z zu Grunde. Bezeichnen wir zwei Punkte P_1 und P_2 durch ihre Coordinaten (x_1, y_1, z_1) und (x_2, y_2, z_2), so wird die Gerade L_{12}, welche diese beiden verbindet, durch den Inbegriff aller Punkte

$$(1) \qquad (\lambda x_1 + \mu x_2, \ \lambda y_1 + \mu y_2, \ \lambda z_1 + \mu z_2)$$

gegeben, wenn das Verhältnis $\lambda : \mu$ alle Werthe von $-\infty$ bis $+\infty$

stetig und reell durchläuft. Jeder Werth von $\lambda : \mu$ bestimmt einen Punkt auf L_{12}; insbesondere werden die Schnittpunkte von L_{12} mit einer Curve, die der Gleichung

$$f(x, y, z) = 0 \tag{2}$$

genügt, durch die Wurzeln von

$$f(\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2) = 0$$

oder, entwickelt nach Potenzen von λ und μ, wenn n die Dimension der homogenen Function f bedeutet,

$$\begin{aligned} 0 = \lambda^n f(x_1, y_1, z_1) &+ \lambda^{n-1}\mu\left[x_2\left(\frac{\partial f}{\partial x}\right)_1 + y_2\left(\frac{\partial f}{\partial y}\right)_1 + z_2\left(\frac{\partial f}{\partial z}\right)_1\right] \\ &+ \frac{\lambda^{n-2}\mu^2}{1\cdot 2}\left[x_2^2\left(\frac{\partial^2 f}{\partial x^2}\right)_1 + 2x_2y_2\left(\frac{\partial^2 f}{\partial x\,\partial y}\right)_1 + \cdots + z_2^2\left(\frac{\partial^2 f}{\partial z^2}\right)_1\right] \\ &+ \cdots \end{aligned} \tag{3}$$

bestimmt. In diesem letzten Ausdrucke verstehen wir die Symbole

$$\left(\frac{\partial f}{\partial x}\right)_1, \cdots \left(\frac{\partial^2 f}{\partial x^2}\right)_1, \left(\frac{\partial^2 f}{\partial x\,\partial y}\right)_1, \cdots$$

so, dass nach der Ausführung der angegebenen Differentiationen die Variablen x, y, z durch x_1, y_1, z_1 zu ersetzen sind.

Wir bezeichnen den in (3) eingehenden Coefficienten von $\frac{\lambda^{n-\alpha}\mu^\alpha}{\alpha!}$ mit

$$\Delta^{(\alpha)}(x_2; f_1) \qquad (\alpha = 0, 1, 2, \cdots n).$$

Dann ist die charakteristische Bedingung dafür, dass P_1 auf der Curve $f = 0$ liegt, durch $\Delta^{(0)}(x_2; f_1) = f(x_1, y_1, z_1) = 0$ gegeben; ferner die Bedingung dafür, dass L_{12} die Curve $f = 0$ in zwei zusammenfallenden Punkten schneidet, durch

$$\Delta^{(0)}(x_2; f_1) = 0, \quad \Delta^{(1)}(x_2; f_1) = 0.$$

Hier tritt nun ein Unterschied ein zwischen den beiden Fällen, dass entweder die drei Grössen

$$\left(\frac{\partial f}{\partial x}\right)_1, \left(\frac{\partial f}{\partial y}\right)_1, \left(\frac{\partial f}{\partial z}\right)_1$$

sämmtlich verschwinden oder nicht. Im zweiten Falle liefert $\Delta^{(1)}(x_2; f_1) = 0$ als lineare, nicht identisch erfüllte Gleichung für x_2, y_2, z_2 aufgefasst, die Tangente an P_1; dagegen ist im ersten Falle $\Delta^{(1)}(x_2; f_1) = 0$ für jedes (x_2, y_2, z_2) befriedigt, d. h. jede L_{12}, die durch (x_1, y_1, z_1) geht, schneidet $f = 0$ in P_1 zweifach. Es ist daher P_1 ein Doppelpunkt für $f = 0$.

Die charakteristische Bedingung dafür, dass L_{12} in P_1 die Curve $f=0$ dreifach schneidet, wird dadurch gegeben, dass (3) den Werth $\mu=0$ als dreifache Wurzel hat, d. h. durch die Erfüllung von

$$\Delta^{(0)}(x_2; f_1)=0, \quad \Delta^{(1)}(x_2; f_1)=0, \quad \Delta^{(2)}(x_2; f_1)=0.$$

Ist nun P_1 ein Doppelpunkt von f, so sind die beiden ersten Bedingungen bereits für jedes x_2, y_2, z_2 erfüllt, und die Bedingung für das dreifache Schneiden reducirt sich darauf, dass x_2, y_2, z_2 die Function $\Delta^{(2)}(x_2; f_1)$ zu Null macht.

Ist P_1 kein Doppelpunkt, dann müssen die durch $\Delta^{(1)}(x_2; f_1)=0$ bestimmten Punkte der Tangente L_{12} sämmtlich $\Delta^{(2)}(x_2; f_1)=0$ befriedigen. Nach § 346, IX ist dies nur möglich, wenn $\Delta^{(1)}$ ein Theiler von $\Delta^{(2)}$ wird.

Wir wollen diese Verhältnisse eingehender untersuchen.

§ 628. Wir setzen dazu der Abkürzung halber

$$\left(\frac{\partial f}{\partial x}\right)_1=r, \quad \left(\frac{\partial f}{\partial y}\right)_1=s, \quad \left(\frac{\partial f}{\partial z}\right)_1=t;$$
$$\left(\frac{\partial^2 f}{\partial x^2}\right)_1=a, \quad \left(\frac{\partial^2 f}{\partial y^2}\right)_1=b, \quad \left(\frac{\partial^2 f}{\partial z^2}\right)_1=c;$$
$$\left(\frac{\partial^2 f}{\partial y\partial z}\right)_1=d, \quad \left(\frac{\partial^2 f}{\partial z\partial x}\right)_1=e, \quad \left(\frac{\partial^2 f}{\partial x\partial y}\right)_1=g;$$

dann liefert uns der Euler'sche Satz über homogene Functionen die Beziehungen

$$\begin{aligned} rx_1+sy_1+tz_1&=nf_1,\\ ax_1+gy_1+ez_1&=(n-1)r,\\ gx_1+by_1+dz_1&=(n-1)s,\\ ex_1+dy_1+cz_1&=(n-1)t. \end{aligned} \tag{4}$$

Setzen wir weiter die sogenannte Hesse'sche Determinante an,

$$H=\begin{vmatrix} a & g & e\\ g & b & d\\ e & d & c \end{vmatrix}=\sum\pm\left(\frac{\partial^2 f}{\partial x^2}\right)_1\left(\frac{\partial^2 f}{\partial y^2}\right)_1\left(\frac{\partial^2 f}{\partial z^2}\right)_1, \tag{4a}$$

so folgt durch Zeilen- und Spaltencombination eine Reihe von sechs Gleichungen

$$\begin{aligned} \frac{H\cdot x_1^2}{(n-1)^2}&=\begin{vmatrix} a & g & r\\ g & b & s\\ r & s & f_1\frac{n}{n-1} \end{vmatrix}, \ \ldots\\ \frac{H\cdot y_1z_1}{(n-1)^2}&=\begin{vmatrix} a & r & e\\ g & s & d\\ r & f_1\frac{n}{n-1} & t \end{vmatrix}, \ \ldots. \end{aligned} \tag{5}$$

Hieraus entnimmt man, dass, wenn, wie bei Doppelpunkten, $r = 0$, $s = 0$, $t = 0$; $f_1 = 0$ ist, dann nach § 341 der Ausdruck

$$\varDelta^{(2)} = ax^2 + 2gxy + 2exz + by^2 + 2dyz + cz^2$$

in zwei lineare Functionen zerfällt. Sind aber nicht alle Coefficienten gleich Null, so giebt es, diesen linearen Functionen entsprechend, zwei durch P_1 gehende Gerade, deren jede in P_1 die Curve $f = 0$ dreifach schneidet. Es sind dies die Tangenten der beiden im Doppelpunkte sich schneidenden Curvenzweige.

Wir wollen weiter den Fall betrachten, dass $f_1 = 0$, $H = 0$ sind, dass aber nicht alle drei Grössen r, s, t zugleich verschwinden. Dann folgt aus (5) zunächst

$$\begin{aligned} ab - g^2 &= -\left(\frac{as - gr}{r}\right)^2 = -\left(\frac{br - gs}{s}\right)^2, \\ bc - d^2 &= -\left(\frac{bt - ds}{s}\right)^2 = -\left(\frac{cs - dt}{t}\right)^2, \\ ca - e^2 &= -\left(\frac{cr - et}{t}\right)^2 = -\left(\frac{at - er}{r}\right)^2; \end{aligned} \tag{6}$$

$$\begin{aligned} dr^2 - ers - grt + ast &= 0, \\ es^2 - gst - dsr + brt &= 0, \\ gt^2 - dtr - ets + crs &= 0. \end{aligned} \tag{7}$$

Wir erhalten, falls $a \neq 0$ und $ab - g^2 \neq 0$ angenommen wird, für $\varDelta^{(2)}(x; f_1) = \varDelta^{(2)}$ die Darstellung

$$\begin{aligned} \varDelta^{(2)} &= \frac{1}{a}(ax + gy + ez)^2 - \frac{1}{a}\left(\frac{as - gr}{r}\right)^2\left(y - \frac{(ad - ge)r^2}{(as - gr)^2}z\right)^2 \\ &= \frac{1}{r}[rx + sy + tz]\cdot\left[ax + \frac{2gr - as}{r}y + \frac{aes - 2ger + adr}{as - gr}z\right], \end{aligned}$$

d. h. $\varDelta^{(2)}$ zerfällt, und

$$\varDelta^{(1)} = rx + sy + tz$$

ist ein Factor von $\varDelta^{(2)}$.

Ist $a \neq 0$ und $ab - g^2 = 0$, so folgt zunächst aus der Identität

$$aH = (ac - e)^2(ab - g^2) - (ad - ge)^2,$$

dass auch $ad - ge = 0$ ist, und ferner ersieht man aus

$$r^2(ab - g^2) = -(as - gr)^2,$$

dass $s = \frac{gr}{a}$ wird. Macht man von beiden Resultaten Gebrauch, so findet man hier als Darstellung von $\varDelta^{(2)}$ die Form

$$\begin{aligned} \varDelta^{(2)} &= \frac{1}{a}\left[ax + gy + ez + \frac{at - er}{r}z\right]\left[ax + gy + ez - \frac{at - er}{r}z\right] \\ &= \frac{1}{r}[rx + sy + tz]\left[ax + gy + \frac{2er - at}{r}z\right], \end{aligned}$$

woraus wiederum folgt, dass $\varDelta^{(1)}$ ein Factor von $\varDelta^{(2)}$ ist.

Gleiches ergiebt sich, wenn b oder c von Null verschieden sind. —

Wären endlich $a, b, c = 0$, so dürften nicht zugleich $d, e, g = 0$ sein, weil sonst $\Delta^{(2)}$ identisch verschwindet; dann zeigt (7) zunächst

$$r(dr - es - gt) = 0,$$
$$s(dr - es - gt) = 0,$$
$$t(dr + es - gt) = 0.$$

Wären nun zwei der Grössen r, s, t gleich Null, etwa die beiden ersten die dritte aber nicht, so würde daraus $g = 0$ folgen, und

$$\Delta^{(1)} = tz, \quad \Delta^{(2)} = 2z(ex + dy)$$

würde wiederum auf das obige Resultat führen.

Wäre dagegen nur eine der Grössen r, s, t gleich Null, etwa r, so folgte $e = 0$, $g = 0$, und das Resultat

$$\Delta^{(1)} = sy + tz, \quad \Delta^{(2)} = 2d \cdot yz$$

schiene in diesem Falle ein anderes zu sein.

Hierbei würde sich aber aus (4) ergeben müssen:

$$sy_1 + tz_1 = 0; \quad d \cdot z_1 = (n-1)s, \quad d \cdot y_1 = (n-1)t;$$
$$(n-1)[sy_1 + tz_1] = 2d \cdot y_1 z_1;$$

es wäre also y_1 oder z_1 gleich Null und daher s oder t gleichfalls, was ausgeschlossen war. Dieser Fall kann demnach nicht eintreten.

Somit erkennen wir:

Aus $f_1 = 0$, $H = 0$ folgt, dass entweder $r = 0$, $s = 0$, $t = 0$ ist, oder dass $\Delta^{(1)}$ ein Factor von $\Delta^{(2)}$ wird.

Tritt das Letzte ein, dann ist (x_1, y_1, z_1) ein Wendepunkt, und

$$\Delta^{(1)}(x_2; f_1) = x_2\left(\frac{\partial f}{\partial x}\right)_1 + y_2\left(\frac{\partial f}{\partial y}\right)_1 + z_2\left(\frac{\partial f}{\partial z}\right)_1 = 0$$

die Wendetangente. Denn wenn man x_2, y_2, z_2 auf $\Delta^{(1)} = 0$ wählt, dann wird auch $\Delta^{(2)}$ zu Null gemacht werden; man hat demgemäss den Schnitt von L_{12} mit $f = 0$ dreifach zu zählen.

Die Dimension von H in x_1, y_1, z_1 beträgt $3(n-2)$, so dass die Anzahl der Wurzeln von

$$f(x, y, z) = 0, \quad H(x, y, z) = 0$$

$3n(n-2)$ wird. Dies ist also auch die Anzahl der Wendepunkte, falls die Curve keine Doppelpunkte besitzt. —

Eine Curve dritter Ordnung ohne Doppelpunkte besitzt neun Wendepunkte.

§ 629. Wir wollen die Schnittpunkte von $f = 0$, $H = 0$ noch genauer untersuchen. Aus (4) folgt, wenn wir die Subdeterminante von H nach der α^{ten} Zeile und der β^{ten} Spalte mit $H_{\alpha\beta}$ bezeichnen, so dass $H_{\alpha\beta} = H_{\beta\alpha}$ ist, für jeden Punkt (x, y, z) der Curve f

$$xH = (n-1)(rH_{11} + sH_{12} + tH_{13}),$$
$$yH = (n-1)(rH_{21} + sH_{22} + tH_{23}),$$
$$zH = (n-1)(rH_{31} + sH_{32} + tH_{33}).$$

Durch Differentiation der ersten dieser Relationen nach y und nach z findet man

$$x\frac{\partial H}{\partial y} = (n-1)\left(r\frac{\partial H_{11}}{\partial y} + s\frac{\partial H_{12}}{\partial y} + t\frac{\partial H_{13}}{\partial y}\right)$$
$$+ (n-1)(gH_{11} + bH_{12} + dH_{13});$$

. . . . ;

hier verschwindet die letzte Klammer wegen (4). Also erhält man

$$(8)\qquad \begin{aligned} x\frac{\partial H}{\partial y} &= (n-1)\left(r\frac{\partial H_{11}}{\partial y} + s\frac{\partial H_{12}}{\partial y} + t\frac{\partial H_{13}}{\partial y}\right),\\ x\frac{\partial H}{\partial z} &= (n-1)\left(r\frac{\partial H_{11}}{\partial z} + s\frac{\partial H_{12}}{\partial z} + t\frac{\partial H_{13}}{\partial z}\right),\end{aligned}$$

und ebenso aus den weiteren Gleichungen

$$(8^a)\qquad \begin{aligned} y\frac{\partial H}{\partial x} &= (n-1)\left(r\frac{\partial H_{21}}{\partial x} + s\frac{\partial H_{22}}{\partial x} + t\frac{\partial H_{23}}{\partial x}\right),\\ y\frac{\partial H}{\partial z} &= (n-1)\left(r\frac{\partial H_{21}}{\partial z} + s\frac{\partial H_{22}}{\partial z} + t\frac{\partial H_{23}}{\partial z}\right),\\ z\frac{\partial H}{\partial x} &= (n-1)\left(r\frac{\partial H_{31}}{\partial x} + s\frac{\partial H_{32}}{\partial x} + t\frac{\partial H_{33}}{\partial x}\right),\\ z\frac{\partial H}{\partial y} &= (n-1)\left(r\frac{\partial H_{31}}{\partial y} + s\frac{\partial H_{32}}{\partial y} + t\frac{\partial H_{33}}{\partial y}\right).\end{aligned}$$

Für die folgende Differentiation benutzen wir die aus

$$0 = gH_{11} + bH_{12} + dH_{13}; \quad H = aH_{11} + gH_{12} + eH_{13}$$

fliessenden Beziehungen

$$\frac{\partial g}{\partial y}H_{11} + \frac{\partial b}{\partial y}H_{12} + \frac{\partial d}{\partial y}H_{13} = -\left(g\frac{\partial H_{11}}{\partial y} + b\frac{\partial H_{12}}{\partial y} + d\frac{\partial H_{13}}{\partial y}\right),$$
$$\frac{\partial a}{\partial y}H_{11} + \frac{\partial g}{\partial y}H_{12} + \frac{\partial e}{\partial y}H_{13} = -\left(a\frac{\partial H_{11}}{\partial y} + g\frac{\partial H_{12}}{\partial y} + e\frac{\partial H_{13}}{\partial y}\right) + \frac{\partial H}{\partial y}.$$

Differentiiren wir nunmehr die erste der Gleichungen (8) nach x, so entsteht

$$x\frac{\partial^2 H}{\partial x\partial y}+\frac{\partial H}{\partial y}=(n-1)\left(r\frac{\partial^2 H_{11}}{\partial x\partial y}+s\frac{\partial^2 H_{12}}{\partial x\partial y}+t\frac{\partial^2 H_{13}}{\partial x\partial y}\right)$$
$$+(n-1)\left(\frac{\partial H}{\partial y}-\left[\frac{\partial a}{\partial y}H_{11}+\frac{\partial g}{\partial y}H_{12}+\frac{\partial e}{\partial y}H_{13}\right]\right)$$

und also

$$(9)\qquad \begin{aligned} x\frac{\partial^2 H}{\partial x\partial y}&=(n-1)\left(r\frac{\partial^2 H_{11}}{\partial x\partial y}+s\frac{\partial^2 H_{12}}{\partial x\partial y}+t\frac{\partial^2 H_{13}}{\partial x\partial y}\right)\\ &-(n-1)\left(\frac{\partial a}{\partial y}H_{11}+\frac{\partial g}{\partial y}H_{12}+\frac{\partial e}{\partial y}H_{13}\right)+(n-2)H.\end{aligned}$$

Ebenso erhalten wir

$$(9^a)\qquad \begin{aligned} x\frac{\partial^2 H}{\partial y\partial z}&=(n-1)\left(r\frac{\partial^2 H_{11}}{\partial y^2}+s\frac{\partial^2 H_{12}}{\partial y^2}+t\frac{\partial^2 H_{13}}{\partial y^2}\right)\\ &-(n-1)\left(\frac{\partial g}{\partial y}H_{11}+\frac{\partial b}{\partial y}H_{12}+\frac{\partial d}{\partial y}H_{13}\right),\end{aligned}$$

und die entsprechenden weiteren Gleichungen.

Jetzt setzen wir $r=0,\ s=0,\ t=0$ voraus und betrachten den Doppelpunkt (x_1, y_1, z_1). Für diesen ergiebt sich dann aus (8) und (8^a), dass $\frac{\partial H}{\partial x}, \frac{\partial H}{\partial y}, \frac{\partial H}{\partial z}$ Null sind; folglich ist (x_1, y_1, z_1) auch ein Doppelpunkt für $H=0$. Ferner ergiebt sich aus (4)

$$x_1 : y_1 : z_1 = H_{\alpha 1} : H_{\alpha 2} : H_{\alpha 3} \qquad (\alpha = 1, 2, 3)$$

und deswegen, mit Berücksichtigung der Gleichheit von $H_{\alpha\beta}$ und $H_{\beta\alpha}$,

$$(10)\qquad \begin{aligned} H_{11}&=N\cdot x_1^2\ , & H_{22}&=N\cdot y_1^2\ , & H_{33}&=N\cdot z_1^2\ ;\\ H_{23}&=N\cdot y_1 z_1, & H_{31}&=N\cdot z_1 x_1, & H_{12}&=N\cdot x_1 y_1.\end{aligned}$$

Geht man mit diesen Resultaten in die Gleichung (9), dann ergiebt sich

$$\begin{aligned} x_1\left(\frac{\partial^2 H}{\partial x\partial y}\right)_1&=-(n-1)N\cdot x_1\left(\left(\frac{\partial a}{\partial y}\right)_1 x_1+\left(\frac{\partial g}{\partial y}\right)_1 y_1+\left(\frac{\partial e}{\partial y}\right)_1 z_1\right)\\ &=-(n-1)N\cdot x_1\left(\left(\frac{\partial g}{\partial x}\right)_1 x_1+\left(\frac{\partial g}{\partial y}\right)_1 y_1+\left(\frac{\partial g}{\partial z}\right)_1 z_1\right)\\ &=-(n-1)(n-2)N\cdot x_1\left(\frac{\partial^2 f}{\partial x\partial y}\right)_1=-(n-1)(n-2)N\cdot x_1 g\end{aligned}$$

und so entsteht endlich

$$\left(\frac{\partial^2 H}{\partial x\partial y}\right)_1=-(n-1)(n-2)N\cdot\left(\frac{\partial^2 f}{\partial x\partial y}\right)_1=-(n-1)(n-2)N\cdot g.$$

Man erhält auf demselben Wege in gleicher Weise auch die entsprechenden Gleichungen und aus ihnen

$$(11)\qquad \left(\frac{\partial^2 H}{\partial x^2}\right)_1 : \left(\frac{\partial^2 H}{\partial x\partial y}\right)_1 : \left(\frac{\partial^2 H}{\partial x\partial z}\right)_1 : \cdots = \left(\frac{\partial^2 f}{\partial x^2}\right)_1 : \left(\frac{\partial^2 f}{\partial x\partial y}\right)_1 : \left(\frac{\partial^2 f}{\partial x\partial z}\right)_1 : \cdots.$$

Nun sind die Glieder der rechten Seite die Coefficienten in $\Delta^{(2)}(x_2; f_1)$; und $\Delta^{(2)}$ bedeutet, wie wir sahen, das Product der linearen Functionen,

die gleich Null gesetzt die Tangenten im Doppelpunkte liefern. Es zeigt daher (11), dass jeder Doppelpunkt von $f=0$ zugleich ein Doppelpunkt von $H=0$ ist, und dass in ihm die Tangenten von $f=0$ mit denen von $H=0$ zusammenfallen.

Legt man den Doppelpunkt in den Nullpunkt $x=0$, $y=0$, so wird mithin

$$f=(a_0x^2+b_0xy+c_0y^2)z^{n-2}+(a_1x^3+\cdots)z^{n-3}+\cdots,$$
$$H=\varepsilon(a_0x^2+b_0xy+c_0y^2)z^{3n-8}+(A_1x^3+\cdots)z^{3n-9}+\cdots;$$

eliminirt man nun etwa y aus den beiden Gleichungen

$$f=0 \quad \text{und} \quad H-\varepsilon f=0,$$

so erkennt man (§ 403), dass jeder Doppelpunkt als sechsfacher Punkt unter den Schnittpunkten von $f=0$ und $H=0$ zu zählen ist*).

Eine Curve dritter Ordnung hat somit entweder einen Doppelpunkt und drei Wendepunkte, oder sie hat neun Wendepunkte.

§ 630. Wir gehen jetzt genauer auf diejenigen Curven dritter Ordnung ein, welche keinen Doppelpunkt und also neun Wendepunkte besitzen.

Legen wir das Coordinatendreieck so, dass der Punkt $x=0$, $y=0$ einer der Wendepunkte und $y=0$ seine Wendetangente ist, so muss $f=0$ für $y=0$ die dreifache Wurzel $x=0$ liefern. Folglich nimmt die Gleichung $f=0$ die Gestalt an

$$(12) \quad f\equiv\alpha x^3+y(3\beta x^2+3\gamma xy+6\delta xz+\varepsilon y^2+3\zeta yz+3\eta z^2)=0.$$

Legt man nun das bisher noch nicht weiter bestimmte Coordinatendreieck so, dass der Eckpunkt $x=0$, $z=0$ gleichfalls ein Wendepunkt und $z=0$ seine Wendetangente wird, dann muss $z=0$ aus der Gleichung $f=0$ wieder die dreifache Wurzel $x=0$ heraustreten lassen. Demnach besitzt f die Form

$$(13) \qquad f\equiv\alpha x^3+3yz(2\delta x+\zeta y+\eta z).$$

Aus dieser entnehmen wir sofort, dass auf $x=0$ noch ein dritter Wendepunkt liegt, in welchem die Wendetangente durch

$$\zeta y+\eta z=0$$

geliefert wird.

Wir wollen dieses Resultat durch unsere Betrachtungen über die

*) Hesse; vgl. Jacobi's Werke 3, p. 545 ff.

Schnitte von $f=0$ und $H=0$ bestätigen. Dabei gehen wir von (12) aus. Wenn dann

$$f(0,y,z)=0,\quad H(0,y,z)=0$$

ausser $y=0$ noch eine zweite Wurzel $y=y_1$ haben, dann müssen sie noch eine dritte Wurzel $y=y_2$ besitzen. Nun ist

$$\frac{1}{6^3}H(0,y,z)=\begin{vmatrix}\beta y & \gamma y+\delta z & \delta y\\ \gamma y+\delta z & \varepsilon y+\zeta z & \zeta y+\eta z\\ \delta y & \zeta y+\eta z & \eta y\end{vmatrix};$$

eine einfache Rechnung liefert

$$\frac{1}{72}H+(\beta\eta-\delta^2)f=(4\beta\varepsilon\eta+6\gamma\delta\zeta-3\beta\zeta^2-4\varepsilon\delta^2-3\eta\gamma^2)y^3;$$

ist also

$$H(0,y_1,z_1)=0,\quad f(0,y_1,z_1)=0\qquad (y_1 \neq 0),$$

dann muss die rechte Seite der vorhergehenden Gleichung identisch verschwinden, und daher stimmen dann, wie behauptet war, $H(0,y,z)$ und $f(0,y,z)$ bis auf einen constanten Factor mit einander überein. Hierdurch ist ein rein algebraischer Beweis des Satzes geliefert, dass die neun Wendepunkte der Curven dritter Ordnung zu je drei auf je einer Geraden liegen, derart, dass vier solcher Geraden durch jeden der neun Wendepunkte gehen.

Wir wollen uns nun mit den Realitätsverhältnissen dieser neun Wendepunkte für reelle Curven beschäftigen. Ist

$$(x,y,z)=(\xi_1+\xi_2 i,\ \eta_1+\eta_2 i,\ \zeta_1+\zeta_2 i)$$

eine Wurzel des Systems $f=0$, $H=0$ mit reellen Coefficienten, dann ist $(x,y,z)=(\xi_1-\xi_2 i,\ \eta_1-\eta_2 i,\ \zeta_1-\zeta_2 i)$ eine Wurzel desselben Systems; die complexen Wurzeln vertheilen sich demnach in Paare conjugirter Wurzeln. Unter den neun Wendepunkten giebt es deshalb mindestens einen reellen. Es sei dies der Punkt $x=0$, $y=0$ und $y=0$ sei in ihm Wendetangente. Dann nimmt die Gleichung $f=0$ die durch (12) gegebene Gestalt an. Hierbei ist die Richtung der Axe $x=0$ noch willkürlich. Wir legen sie so, dass sie durch einen zweiten und also auch durch einen dritten reellen oder imaginären Wendepunkt geht. Ist dabei für diesen die Wendetangente durch

$$Ax+By+Cz=0 \tag{14}$$

mit reellen oder complexen Coefficienten gegeben, dann muss die Eintragung von (14) in (12) die dreifache Wurzel $x=0$ liefern. Folglich ist die Klammergrösse rechts in (12) durch das Polynom von (14) theilbar.

Somit erkennt man, dass, wenn auf $x = 0$ drei Wendepunkte mit den Wendetangenten

$$y = 0, \quad Ax + By + Cz = 0, \quad A_1 x + B_1 y + C_1 z = 0$$

liegen, dann f die Gestalt annimmt

$$(15) \qquad f \equiv \alpha x^3 + y(Ax + By + Cz)(A_1 x + B_1 y + C_1 z).$$

Nun wollen wir annehmen, dass der zweite und der dritte dieser Wendepunkte imaginär sind. Dann zeigt die letzte Gleichung, dass die beiden letzten Factoren conjugirt complex werden, also etwa, nach Division durch A und A_1,

$$x + (m + ni)y + (p + qi)z, \quad x + (m - ni)y + (p - qi)z;$$

ihr Product ergiebt dann

$$(x + my + pz)^2 + (ny + qz)^2,$$

und wenn man statt $my + pz$ eine neue z-Coordinate einführt,

$$f \equiv \alpha x^3 + y[(ny + qz)^2 + (x + q_1 z)^2].$$

Dies ist das Polynom der Curvengleichung, falls auf $x = 0$ neben einem reellen zwei imaginäre Wendepunkte liegen.

Hat $f = 0$ mehr als einen reellen Wendepunkt, so giebt es deren mindestens drei. Dass dies eintritt, ist auf rein algebraischem Wege ohne Verwendung der Invariantentheorie nur durch umständliche Rechnungen zu zeigen.

Wir übergehen diese und weisen hier auf die geometrischen Ueberlegungen hin, wie sie sich z. B. in den Vorlesungen über Geometrie von Clebsch (herausgegeben von Lindemann) I, p. 499 befinden.

Hiernach haben die reellen Curven dritter Ordnung ohne Doppelpunkt mindestens drei reelle Wendepunkte.

Legen wir diese drei nun auf die $x = 0$ Axe, so können wir die Gestalt (13) für f zu Grunde legen, oder indem wir neue, den alten proportionale Coordinaten einführen,

$$f \equiv \alpha x^3 + yz(x + y + z).$$

Hierfür wird

$$\begin{aligned} \tfrac{1}{2} H = (z - 12\alpha x)y^2 + (z^2 + (1 - 12\alpha)xz - 12\alpha xz)y \\ - (3\alpha x^3 + 12\alpha x^2 z + 12\alpha x z^2), \end{aligned}$$

$$(24\alpha x - 2z) \cdot f + zH = 8\alpha x(3\alpha x^3 - zx^2 - 3z^2 x - 3z^3).$$

Der letzte Ausdruck zeigt, dass die Eliminante von f und H nur die Factoren rechts enthalten kann, von denen der zweite irreductibel ist. Da der erste bereits als dreifache Wurzel bekannt ist, so folgt

$$R_{f,H} = x^3(3\alpha x^3 - zx^2 - 3z^2 x - 3z^3)^2.$$

Der zweite Factor verschwindet für eine und nur eine reelle Wurzel $x = x_1$, da ja die Gleichung dritten Grades

$$3\alpha x^3 - zx^2 - 3z^2x - 3z^3 = 0$$

vorliegt, für welche die Discriminante

$$D = -\frac{(1+27\alpha)^2 z^6}{3^6\alpha^4}$$

negativ ist (§ 216, Bd. I).

Aber für diese reelle Wurzel x_1 liefert

$$f(x_1, y, z) \equiv y^2z + (x_1 + z)yz + \alpha x_1^3 = 0$$

nur complexe Wurzeln y. Denn ihre Discriminante können wir

$$-4\alpha x_1^3 z + (x_1 + z)^2z^2 = -\frac{4z}{3}(zx_1^2 + 3z^2x_1 + 3z^3) + (x_1 + z)^2z^2$$
$$= -\frac{1}{3}(x_1z + 3z^2)^2$$

setzen; sie ist also negativ.

Daraus entnehmen wir auf algebraischem Wege, dass von den neun Wendepunkten einer Curve dritter Ordnung stets drei und nur drei reell sind.

Jede Gerade, auf welcher drei der neun Wendepunkte liegen, heisst eine Wendepunktsgerade. Auf jeder reellen Wendepunktsgeraden liegen ein oder drei reelle Wendepunkte. Die beiden conjugirt complexen Wendepunkte

$$(x, y, z) = (m + ni, p + qi, z); \quad (x, y, z) = (m - ni, p - qi, z)$$

liegen auf der reellen Wendepunktsgeraden

$$qx - ny + (np - qm)z = 0;$$

diese geht also durch einen der drei reellen Wendepunkte hindurch. Für jeden reellen Wendepunkt werden demnach von den vier in ihm sich schneidenden Wendepunktsgeraden mindestens zwei reell sein. Wir wollen nachweisen, dass die beiden übrigen imaginär sind. Zu dem Zwecke legen wir das Coordinatendreieck so, wie es durch

$$(13) \qquad f \equiv \alpha x^3 + 3yz(2\delta x + \zeta y + \eta z)$$

festgesetzt war. Ist nun noch eine zweite durch $x = 0$, $y = 0$ gehende Gerade $x - \varrho y = 0$ eine Wendepunktsgerade, so muss auch

$$f \equiv \alpha_1(x - \varrho y)^3 + g_1(x, y, z) \cdot g_2(x, y, z) \cdot g_3(x, y, z)$$

sein, wobei die $g_\alpha = 0$ lineare homogene Gleichungen sind, welche die Wendepunktstangenten liefern. Diejenige, welche zu $x = 0$, $y = 0$ gehört, wird aber zu $y = 0$; also können wir schreiben

$$f \equiv \alpha_1(x - \varrho y)^3 + y \cdot g_2(x, y, z) \cdot g_3(x, y, z);$$

es folgt dies übrigens auch rein algebraisch aus der Vergleichung der Coefficienten in den beiden letzten Formen für f. Auf demselben Wege erkennt man, dass $\alpha_1 = \alpha$ ist.

Es wird folglich $x - \varrho y = 0$ eine Wendepunktsgerade, wenn

$$[\alpha x^3 - \alpha(x - \varrho y)^3 + 3yz(3\delta x + \zeta y + \eta z)] : y$$

in zwei lineare Factoren g_2 und g_3 zerlegbar ist. Nach § 341 ist die Bedingung dafür

$$\begin{vmatrix} 2\alpha\varrho & -3\alpha\varrho^2 & 2\delta \\ -\alpha\varrho^2 & 2\alpha\varrho^3 & \zeta \\ 2\delta & 3\zeta & 2\eta \end{vmatrix} = 0$$

oder nach Unterdrückung des Factors $2\alpha\varrho$, der nur $x = 0$ giebt,

$$(16) \qquad \alpha\eta\varrho^3 + 4\delta^2\varrho^2 + 6\delta\zeta\varrho + 3\zeta^2 = 0.$$

Die Discriminante dieser Gleichung lautet

$$-\left[\frac{8\delta^3\zeta}{3\alpha^2\eta^2} - 3\frac{\zeta^2}{\alpha\eta}\right]^2;$$

es giebt also nur eine reelle Wurzel für (16), d. h. ausser $x = 0$ nur noch eine reelle Wendepunktsgerade durch $(0, 0, z)$.

Durch jeden reellen Wendepunkt gehen also zwei reelle und zwei imaginäre Wendepunktsgerade. Auf der einen reellen liegen die drei reellen Wendepunkte; auf der anderen liegt ein Paar conjugirt-complexer Wendepunkte. Es giebt also vier reelle Wendepunktsgerade; eine, welche die drei reellen Wendepunkte enthält; und drei, von denen jede zwei conjugirt-complexe und einen der reellen Wendepunkte verbindet. Ausser diesen giebt es keine reellen Wendepunktsgeraden. Denn gäbe es noch eine reelle, so müsste diese in ihrem Schnitte mit $f = 0$ einen reellen Wendepunkt liefern, was nach dem eben Dargelegten nicht möglich ist.

Die drei Wendepunktsgeraden, welche je zwei conjugirt-complexe Wendepunkte verbinden, bilden ein reelles Dreieck, auf dessen Seiten sämmtliche neun Wendepunkte liegen.

§ 631. Wir wollen nun die Wendepunkte mit $1, 2, 3, \cdots 8, 9$ bezeichnen und die durch sie gebildete Configuration untersuchen.

Auf der Geraden L_{12} liegt noch ein Wendepunkt, den wir mit 3 bezeichnen wollen; dann sagen wir, dass die Punkte 1, 2, 3 ein Tripel (1, 2, 3) bilden. Auf L_{14} liegt ein weiterer Punkt; er heisse 5; so entsteht das Tripel (1, 4, 5). Auf L_{24} kann nun weder 1 noch 3 noch 5 liegen; wir nennen den auf L_{24} befindlichen Punkt 6 und

haben somit das Tripel (2, 4, 6). Ebenso kann wegen der drei schon vorhandenen Tripel die Gerade L_{16} keinen der Punkte 2, 3, 4, 5 enthalten; den auf ihr liegenden neuen nennen wir 7 und haben das Tripel (1, 6, 7). Daraus folgt sofort das Tripel (1, 8, 9). Aus der Existenz von

$$(1, 2, 3), \quad (1, 4, 5), \quad (1, 6, 7), \quad (1, 8, 9), \quad (2, 4, 6)$$

ergiebt sich, dass L_{25} nur einen der Punkte 7, 8, 9 enthalten kann; käme aber 7 darauf vor, so würde zu dem Tripel (2, 5, 7) noch (2, 8, 9) treten. Dann lägen aber wegen (1, 8, 9) auf L_{89} die beiden Punkte 1 und 2, was unmöglich ist. Somit liegt auf L_{25} entweder 8 oder 9. Da man aber in den vorhandenen Tripeln 8 mit 9 vertauschen kann, so ist es keine Einschränkung, (2, 5, 8) anzunehmen, woraus dann (2, 7, 9) folgt. Für L_{47} ergiebt sich dann eine der beiden Möglichkeiten für die Tripelbildung: (4, 7, 3) und (4, 7, 8). Da die erste derselben (4, 8, 9) im Gefolge haben würde, weil für 4 nur noch die beiden freien Punkte 8 und 9 übrig blieben, und weil dieses Tripel gegen (1, 8, 9) verstiesse, so bleibt (4, 7, 8), dem sich dann als Ergänzungen (3, 4, 9) und (3, 5, 7) anschliessen. Dadurch ergeben sich sofort und unzweideutig die übrigen Tripel.

Man erhält also die bis auf ihre Bezeichnung eindeutige Vertheilung

$$(17)\quad \begin{array}{l} (1, 2, 3),\ (4, 7, 8),\ (5, 6, 9);\ \ (1, 4, 5),\ (2, 7, 9),\ (3, 6, 8); \\ (1, 6, 7),\ (2, 5, 8),\ (3, 4, 9);\ \ (1, 8, 9),\ (2, 4, 6),\ (3, 5, 7). \end{array}$$

Die Anordnung in je drei Tripel ist hier so getroffen, dass jedesmal alle neun Wendepunkte vorkommen. Da nun ein jedes Tripel (a, b, c) einer Wendepunktsgeraden L_{abc} entspricht, so sehen wir, dass vier **Wendepunktsdreiecke** bestehen, die von

$$(L_{123}, L_{478}, L_{569});\quad (L_{145}, L_{279}, L_{368});$$
$$(L_{167}, L_{258}, L_{349});\quad (L_{189}, L_{246}, L_{357})$$

gebildet werden.

Die Darstellung (17) ist nicht übersichtlich. Man erhält eine klarere Vertheilung, wenn man jeden der Punkte durch zwei Indices bezeichnet, etwa

$$1 = 00;\quad 2 = 11;\quad 3 = 22;\quad 4 = 01;\quad 5 = 02;\quad 6 = 21;$$
$$7 = 12;\quad 8 = 20;\quad 9 = 10;$$

dann entstehen die Tripel

$$(17^{a})\quad \begin{array}{lll} (00, 11, 22), & (01, 12, 20), & (02, 10, 21); \\ (00, 01, 02), & (10, 11, 12), & (20, 21, 22); \\ (00, 12, 21), & (02, 11, 20), & (01, 10, 22); \\ (00, 10, 20), & (01, 11, 21), & (02, 12, 22). \end{array}$$

Diese sind dadurch gekennzeichnet, dass $(a_1 b_1, a_2 b_2, a_3 b_3)$ dann und nur dann ein Tripel ist, falls

$$(18) \qquad a_1 + a_2 + a_3 \equiv 0, \quad b_1 + b_2 + b_3 \equiv 0 \quad (\text{mod. } 3)$$

wird. Jedem Paare $a_1 b_1, a_2 b_2$ entspricht dabei durch die Bedingung (18) ein von jenen beiden verschiedenes System $a_3 b_3$, falls nur die beiden ersten unter sich verschieden sind.

§ 632. Sind die beiden in § 627 betrachteten Punkte P_1 und P_2 Wendepunkte der Curve $f(x, y, z) = 0$ von dritter Ordnung, so findet man den dritten auf L_{12} liegenden Wendepunkt durch die Bestimmung des Quotienten $\lambda : \mu$ aus der Gleichung (3), welche im vorliegenden Falle, in dem P_1 und P_2 auf $f = 0$ liegen, die besonders einfache Gestalt annimmt

$$\lambda \cdot \Delta^{(1)}(x_2; f_1) + \mu \Delta^{(1)}(x_1; f_2) = 0.$$

Es wird daher

$$(19) \qquad \frac{\mu}{\lambda} = -\frac{x_2 \left(\frac{\partial f}{\partial x}\right)_1 + y_2 \left(\frac{\partial f}{\partial y}\right)_1 + z_2 \left(\frac{\partial f}{\partial z}\right)_1}{x_1 \left(\frac{\partial f}{\partial x}\right)_2 + y_1 \left(\frac{\partial f}{\partial y}\right)_2 + z_1 \left(\frac{\partial f}{\partial z}\right)_2}.$$

Führen wir demnach in die beiden Gleichungen

$$f(x, y, z) = 0, \quad H(x, y, z) = 0$$

durch die lineare Substitution

$$u = \varrho_1 x + \varrho_2 y; \quad y = \frac{u - \varrho_1 x}{\varrho_2}$$

an Stelle von y die Grösse u ein und eliminiren aus den Resultaten

$$f\left(x, \frac{u - \varrho_1 x}{\varrho_2}, z\right) = 0, \quad H\left(x, \frac{u - \varrho_1 x}{\varrho_2}, z\right) = 0$$

die Unbekannte x, so wird die Eliminante, abgesehen von einer Potenz von z, als Wurzelstellen die neun Werthe von u haben, welche diese Grösse für die neun Wendepunkte von $f = 0$ annimmt. Diese Wurzeln bezeichnen wir gemäss unseren Festsetzungen mit $u_{00}, u_{01}, u_{02}; \cdots u_{20}, u_{21}, u_{22}$. Durch (17[a]) wird die Zugehörigkeit von je dreien zu je einer Wendepunktsgeraden festgelegt, und aus (19) entnehmen wir, dass jedes $u_{a_3 b_3}$ eines Tripels durch die $u_{a_1 b_1}$ und $u_{a_2 b_2}$ des gleichen Tripels rational darstellbar ist. Die Form von (19) zeigt zugleich, dass durch dieselbe rationale Function R

$$(20) \qquad u_{a_3 b_3} = R(u_{a_1 b_1}, u_{a_2 b_2}) = R(u_{a_2 b_2}, u_{a_1 b_1})$$

jedes u jedes einzelnen Tripels durch die beiden anderen u desselben Tripels dargestellt werden kann.

§ 633. Wir sind durch diese Betrachtungen auf algebraische Gleichungen besonderen Charakters gelangt*): Wir nennen eine Gleichung ohne gleiche Wurzeln eine Tripelgleichung, wenn ihre Wurzeln in Tripel zu je drei derart eingetheilt werden können, dass zwei Wurzeln $u_{a_1 b_1}$ und $u_{a_2 b_2}$ jeden Tripels beliebig wählbar sind, und die dritte $u_{a_3 b_3}$ aus diesen beiden durch eine rationale Function

$$(20) \qquad u_{a_3 b_3} = R(u_{a_1 b_1}, u_{a_2 b_2}) = R(u_{a_2 b_2}, u_{a_1 b_1})$$

eindeutig bestimmt wird. In (20) sind dabei also die Wurzeln eines Tripels beliebig mit einander vertauschbar.

Tripelgleichungen giebt es nur von einem Grade $n = 6m + 1$ oder $n = 6m + 3$. Denn mit n Wurzeln kann man überhaupt $\frac{n(n-1)}{2}$ Combinationen von je zwei Wurzeln bilden. Zu jeder dieser Combinationen gehört eine dritte, welche das Tripel vervollständigt. Je drei der so erhaltenen Tripel enthalten dabei dieselben Elemente; folglich kommen $\frac{n(n-1)}{6}$ verschiedene Tripel vor; und daraus folgt, dass $n = 6m + 1$ oder $6m + 3$ sein muss. Denn die Möglichkeit $n = 6m$ ist auszuschliessen, da n ungerade sein muss, wie man erkennt, wenn man ein Element mit allen übrigen verbindet.

Die Aufgabe der Bildung von Tripelsystemen stammt von T. P. Kirkmann**) und von J. Steiner***). Den Nachweis dafür, dass es für jedes $n = 6m + 1$ und $n = 6m + 3$ Tripelsysteme gäbe, sowie eine Construction, welche für alle Fälle ausreicht, lieferte M. Reiss†).

Abgesehen von $n = 3$ liefert $n = 7$ das einfachste Tripelsystem. Es ist dies

$$(21) \qquad \begin{gathered}(1, 2, 3), \quad (1, 4, 5), \quad (1, 6, 7), \quad (2, 4, 6), \quad (2, 5, 7), \\ (3, 4, 7), \quad (3, 5, 6);\end{gathered}$$

und dies ist, wie man bei der Construction leicht erkennt, abgesehen von der Bezeichnung auch das einzig mögliche.

Für $n = 13$ giebt es zwei††) und auch nur zwei Tripelsysteme†††), welche wesentlich von einander verschieden sind.

---

*) O. Hesse, Journ. f. Math. 34 (1847), p. 193.

**) Cambr. and Dublin math. Journ. 7 (1852), p. 527 und 8 (1853), p. 38.

***) Journ. f. Math. 45 (1853), p. 181 = Werke 2, p. 435.

†) Journ. f. Math. 56 (1859), p. 326.

††) K. Zulauf, „Ueber Tripelsysteme von 13 Elementen", Dissert. Giessen 1897.

†††) V. de Pasquale, Rendic. R. Istit. Lombardo 1899.

§ 634. Wir wollen uns zunächst mit der Gruppe der Tripelgleichungen siebenten Grades beschäftigen.

Eine Substitution zwischen den sieben Wurzeln der Gleichung, welche wir kurz durch die Zahlen $1, 2, \cdots 6, 7$ bezeichnen wollen, kann nur dann zur Gruppe gehören, wenn sie die Tripel (21) lediglich unter einander umstellt; denn die rationale Beziehung (20) darf durch Substitutionen der Galois'schen Gruppe nicht gestört werden.

Lässt eine Substitution der Gruppe demnach zwei Elemente ungeändert, so lässt sie auch das dritte, jene zwei zu einem Tripel ergänzende ungeändert.

Lässt sie ausser den drei eines Tripels noch eine weitere Wurzel an ihrer Stelle, so ändert sie überhaupt keine Wurzel; das erkennt man sofort aus der Configuration von (21).

Folglich giebt es nur Substitutionen, die kein Element ungeändert lassen; solche, die ein Element nicht umstellen; solche, die drei Elemente ungeändert lassen und endlich noch die Einheit.

Wir suchen zunächst diejenigen Substitutionen, welche $1, 2, 3$ nicht umstellen. Diese können nur

$$(1, 4, 5) \text{ und } (1, 6, 7); \quad (2, 4, 6) \text{ und } (2, 5, 7); \quad (3, 4, 7) \text{ und } (3, 5, 6)$$

in einander umwandeln. Alle hierbei überhaupt vorhandenen Möglichkeiten genügen den Anforderungen:

$$s_1 = (45)(67), \quad s_2 = (46)(57), \quad s_3 = (47)(56).$$

Derartige drei Substitutionen entsprechen jedem Tripel aus (21). Neun unter diesen 21 enthalten das Element 1 nicht.

Wir suchen ferner alle Substitutionen, die 1 nicht bewegen, dagegen alle anderen Wurzeln unter einander vertauschen. Diese können nur

$$(22) \qquad (1, 2, 3), \quad (1, 4, 5), \quad (1, 6, 7)$$

unter sich, und ebenso

$$(23) \qquad (2, 4, 6), \quad (2, 5, 7), \quad (3, 4, 7), \quad (3, 5, 6)$$

unter sich umstellen. Alle hierbei überhaupt vorhandenen Möglichkeiten genügen den Anforderungen. Zuerst ergeben sich diejenigen, welche eins der Tripel (22) in sich verwandeln:

$$t_1 = (23)(4657), \quad t_2 = (45)(2736), \quad t_3 = (67)(2435);$$
$$t_1^3 = (23)(4756), \quad t_2^3 = (45)(2637), \quad t_3^3 = (67)(2534);$$

dann diejenigen, welche die Tripel (22) cyklisch unter einander vertauschen:

$$u_1 = (246)(357), \quad u_2 = (247)(356), \quad u_3 = (256)(347), \quad u_4 = (257)(346);$$
$$u_1^2 = (264)(375), \quad u_2^2 = (274)(365), \quad u_3^2 = (265)(374), \quad u_4^2 = (275)(364).$$

Die Anzahl der Substitutionen, welche alle Elemente umstellen, können wir mit Hülfe der in § 572 aufgestellten Formel

$$n\left(\frac{1}{2}[n-2]+\frac{2}{3}[n-3]+\cdots+\frac{n-1}{n}[0]\right)$$

berechnen. Hier ist $[n-3]$, wie eben gezeigt wurde, gleich 9; $[0]$ ist gleich 1; die übrigen eckigen Klammern sind sämmtlich gleich Null. Danach erhalten wir

$$7\left(\frac{2}{3}\cdot 9+\frac{6}{7}\cdot 1\right)=48$$

Substitutionen, welche kein Element an seiner Stelle lassen. Jede dieser Substitutionen muss cyklisch sein, weil sonst eine geeignete Potenz entweder nur fünf oder drei oder zwei Elemente umsetzen würde. Aus der Combination der s und der t oder der u findet man leicht solche Substitutionen. Wir wählen

$$v_1=(1243675),\quad v_2=(1245736).$$

Transformirt man v_1 durch $v_2, v_2^2, \cdots v_2^6$, so erhält man noch sechs andere cyklische Substitutionen von sieben Elementen $v_3, v_4, \cdots v_8$, und die $6\cdot 8$ verschiedenen Potenzen der $v_1, \cdots v_8$ liefern die nothwendigen noch fehlenden Substitutionen der Gruppe.

Die Ordnung der Gruppe beträgt nach § 572

$$7\{[6]+[5]+\cdots+[0]\}=7\cdot(14+9+1)=168.$$

Diese Gruppe hat Kronecker angegeben. Sie ist zweifach transitiv.

Die Galois'sche Gruppe jeder Tripelgleichung siebenten Grades ist mit der gefundenen Gruppe identisch oder ein Theiler derselben.

§ 635. Nach diesem Excurs kehren wir zu den Tripelgleichungen neunten Grades zurück und suchen ihre Galois'sche Gruppe zu bestimmen. Für die Bezeichnung der Wurzeln legen wir, genau wie in (17^a), zwei Indices zu Grunde. Eine Substitution kann nur dann zur Galois'schen Gruppe der Gleichung gehören, wenn sie die Tripel (17^a) nur unter einander vertauscht.

Wir betrachten nun alle Substitutionen von der Form

$$(24)\qquad s=\left|\, h, k \quad ah+bk+\alpha,\; a_1h+b_1k+\alpha_1 \,\right|.$$

Wendet man sie auf das Tripel

$$(h_1k_1,\, h_2k_2,\, h_3k_3)\qquad (h_1+h_2+h_3\equiv k_1+k_2+k_3\equiv 0)$$

an, so wird erstens

$$a\Sigma h+b\Sigma k+3\alpha\equiv a_1\Sigma h+b_1\Sigma k+3\alpha_1\equiv 0\quad (\text{mod. } 3)$$

sein; d. h. jedes s führt die Tripel in einander über.

Umgekehrt muss jede Substitution, welche die Tripel in einander überführt, die Form (24) besitzen, wie wir jetzt zeigen wollen.

Zunächst entnehmen wir aus (17), dass, wenn die Elemente 1, 2, 4 fest bleiben, der Reihe nach wegen

(1, 2, 3) auch 3; wegen (1, 4, 5) auch 5; wegen (2, 4, 6) auch 6, ⋯

u. s. f. ungeändert bleiben. Eine Substitution also, die 1, 2, 4 nicht ändert, ist die identische Substitution; übertragen wir dies auf (17ª), so folgt, dass wenn eine Substitution der Galois'schen Gruppe die Elemente 00, 11, 01 nicht ändert, sie gleich der Einheit wird.

Nun sei t eine beliebige Substitution der Galois'schen Gruppe. Sie lasse auf

$$00,\ 11,\ 01 \quad \text{folgen} \quad pq,\ p_1q_1,\ p_2q_2.$$

Wir bilden das zur Gruppe gehörige

$$s_\alpha = \left| h, k \quad (p_1 - p_2)h + (p_2 - p)k + p,\ (q_1 - q_2)h + (q_2 - q)k + q \right|;$$

dann wird $t \cdot s_\alpha^{-1}$ die drei Elemente 00, 11, 01 nicht ändern und folglich gleich der Einheit sein, d. h. es ist das beliebige t gleich einem s_α von der Form (24).

Damit ist gezeigt, dass alle Substitutionen, welche die Tripel (17ª) in einander umwandeln und nur sie durch die linearen Substitutionen (24) gegeben sind.

In (24) können die a, b, a_1, b_1 auf $(3^2 - 1)(3^2 - 3) = 48$ verschiedene Arten so gewählt werden, dass (24) eine von 0 verschiedene Determinante hat (§ 531); α und α_1 können gleich 0, 1, 2 angenommen werden. Folglich hat die Gruppe die Ordnung $9 \cdot 48$.

Eine Gleichung mit dieser Gruppe ist algebraisch auflösbar. Man könnte dies durch unsere früheren Resultate über auflösbare Gleichungen der Grade p^2 hier ableiten, doch wir ziehen einen direkten Nachweis vor, weil bei diesem die Bedeutung der einzelnen Schritte, welche zur Lösung führen, deutlicher heraustritt.

Es handelt sich natürlich um die Frage nach der Composition der durch die Substitutionen (24) bestimmten Gruppe, die wir G nennen wollen.

Zunächst bemerken wir, dass die Substitutionen

$$| h, k \quad k + \alpha,\ k + \alpha_1 |$$

lediglich jede der Wendepunktsgeraden (17ª) in eine solche des Dreiecks

$$\begin{aligned}
\text{I} &= [(00,\ 11,\ 22);\ (01,\ 12,\ 20);\ (02,\ 10,\ 21)],\\
\text{II} &= [(00,\ 01,\ 02);\ (10,\ 11,\ 12);\ (20,\ 21,\ 22)],\\
\text{III} &= [(00,\ 12,\ 21);\ (02,\ 11,\ 20);\ (01,\ 10,\ 22)],\\
\text{IV} &= [(00,\ 10,\ 20);\ (01,\ 11,\ 21);\ (02,\ 12,\ 22)]
\end{aligned}$$

umwandelt, dem sie selbst angehört. Zu jeder Substitution von G ordnen sich also je nach den Werthen von α und α_1 noch acht andere zu, denen dieselbe Umstellung der Dreiecke I, II, III, IV entspricht. Es reicht daher aus, nur die Substitutionen mit $\alpha = \alpha_1 = 0$ zu betrachten; diese bilden eine Gruppe G_1, zu welcher G neunstufig isomorph ist. G_1 hat die Ordnung 48.

Jede Substitution aus G_1 kann man als Umsetzung der Dreiecke I, II, III, IV deuten. Es ist also G_1 der dadurch hervorgerufenen Gruppe Γ unter den Elementen I, II, III, IV isomorph. Man überzeugt sich leicht, dass

$$s = | h, k \quad 2h, 2k | \pmod{3}$$

nebst der Einheit die einzigen Substitutionen von G_1 werden, welche alle Dreiecke ungeändert lassen. Denn jede Substitution von G_1 lässt 00 ungeändert; soll sie nun I und II nicht ändern, so muss sie 11 in sich oder in 22, und 01 in sich oder in 02 umwandeln. Durch (25) kommt man dann auf das angegebene Resultat, da von den vier möglichen Combinationen nur jene befriedigt.

Somit ist G_1 zu Γ zweistufig isomorph; Γ hat die Ordnung 24 und ist deshalb die symmetrische Gruppe der vier Elemente I, II, III, IV.

In Γ ist die alternirende Gruppe A ein autojuger Maximaltheiler mit dem Compositionsfactor 2. Der Gruppe A entspricht in G_1 die Gruppe A von 24 Substitutionen, welche sämmtlich die Dreiecke so unter einander vertauschen, dass gerade Permutationen entstehen, d. h. solche, die durch eine gerade Anzahl von Transpositionen bewirkt werden können.

In A bildet die Gruppe

$$(\mathrm{I\ II})(\mathrm{III\ IV}), \quad (\mathrm{I\ III})(\mathrm{II\ IV}), \quad (\mathrm{I\ IV})(\mathrm{II\ III}), \quad 1$$

einen autojugen Maximaltheiler K. Ihr entspricht in A eine Gruppe K der Ordnung 8, da der Compositionsfactor gleich 3 wird. Ihre Substitutionen sind

$$\begin{gathered} 1, \quad | h, k \quad k, 2h |, \quad | h, k \quad 2h, 2k |, \quad | h, k \quad 2k, h |; \\ | h, k \quad h + 2k, 2h + 2k |, \quad | h, k \quad h + k, h + 2k |, \\ | h, k \quad 2h + k, h + k |, \quad | h, k \quad 2h + 2k, 2h + k |. \end{gathered}$$

Von ihr aus geht man mit dem Compositionsfactor 2 zu dem aus den vier ersten Substitutionen gebildeten autojugen Theiler über und von da zu

$$1, \quad | h, k \quad 2h, 2k |,$$

d. h. zu den einzigen Substitutionen aus G_1, welche alle Dreiecke I,

II, III, IV nicht ändern. In G haben diese Eigenschaft die 18 Substitutionen

$$|\,h, k \quad h+\alpha, k+\alpha_1\,|, \quad |\,h, k \quad 2h+\alpha, 2k+\alpha_1\,|.$$

Durch Vermittelung von Compositionsfactoren 2, 3, 2, 2, 2 gelangt man also von G zu der arithmetischen Gruppe

$$|\,h, k \quad h+\alpha, \quad k+\alpha_1\,|.$$

Folglich ist die Tripelgleichung, wie behauptet worden war, algebraisch auflösbar.

§ 636. Wir haben bereits erwähnt, dass im Falle von 13 Elementen zwei wesentlich verschiedene Arten von Tripelsystemen existiren. Das erste wurde von Reiss (l. c.) aufgestellt; bezeichnen wir die Elemente mit 0, 1, $\cdots$ 9, a, b, c, so kann es durch

$(0, 1, a)$, $(0, 2, 4)$, $(0, 3, 9)$, $(0, 5, b)$, $(0, 6, c)$, $(0, 7, 8)$,
$(1, 2, 3)$, $(1, 4, 5)$, $(1, 6, 8)$, $(1, 7, c)$, $(1, 9, b)$, $(2, 5, 6)$,
$(2, 7, 9)$, $(2, 8, a)$, $(2, b, c)$, $(3, 4, a)$, $(3, 5, 7)$, $(3, 6, b)$,
$(3, 8, c)$, $(4, 6, 7)$, $(4, 8, b)$, $(4, 9, c)$, $(5, 8, 9)$, $(5, a, c)$,
$(6, 9, b)$, $(7, a, b)$

dargestellt werden. Seine Gruppe, d. h. die Gesammtheit der Substitutionen, welche diese Tripel nur unter einander umwandeln, wird

$$1,\ (0,1,2)(3,4,a)(5,8,9)(6,7,b),\ (0,2,1)(3,a,4)(5,9,8)(6,b,7);$$
$$(0,7)(1,6)(2,b)(4,a)(5,9),\ (0,6)(1,b)(2,7)(3,a)(5,8),$$
$$(0,b)(1,7)(2,6)(3,4)(8,9);$$

hier bilden die ersten drei einen autojugen Theiler; folglich ist die Gruppe auflösbar. —

Das zweite Tripelsystem von 13 Elementen habe ich in den Math. Ann. 42 (1892), p. 143 sowie in meiner Substitutionentheorie (1882) § 220 behandelt. Es wird durch die Tripel

$(0, 1, a)$, $(0, 2, 7)$, $(0, 3, 4)$, $(0, 5, b)$, $(0, 6, 8)$, $(0, 9, c)$,
$(1, 2, b)$, $(1, 3, 8)$, $(1, 4, 5)$, $(1, 6, c)$, $(1, 7, 9)$, $(2, 3, c)$,
$(2, 4, 9)$, $(2, 5, 6)$, $(2, 8, a)$, $(3, 5, a)$, $(3, 6, 7)$, $(3, 9, b)$,
$(4, 6, b)$, $(4, 7, 8)$, $(4, a, c)$, $(5, 7, c)$, $(5, 8, 9)$, $(6, 9, a)$,
$(7, a, b)$, $(8, b, c)$

und seine Gruppe G durch die $3 \cdot 13$ Combinationen der beiden Substitutionen

$$s = (0,\ 1,\ 2,\ 3, \cdots 9,\ a,\ b,\ c),$$
$$t = (1,\ 3,\ 9)(2,\ 6,\ 5)(4,\ c,\ a)(7,\ 8,\ b)$$

gebildet. Die Potenzen von s sind autojug in G; G ist also auflösbar.

So zeigt es sich: Die Tripelgleichungen 13[ten] Grades sind auflösbar.

Siebenundsechzigste Vorlesung.

Die auflösbaren Gleichungen fünften Grades.

§ 637. Wir haben gesehen, dass es für eine auflösbare irreductible Gleichung fünften Grades charakteristisch ist, eine und damit alle metacyklischen Functionen im Rationalitätsbereiche zu besitzen. Eine solche metacyklische Function hängt nun, da bei $p = 5$ die Gruppe von der Ordnung 20 ist, von einer Gleichung des Grades $\frac{5!}{20} = 6$ ab; es ist also charakteristisch, dass diese Gleichung eine rationale Wurzel besitzt, und dass die Gleichung fünften Grades irreductibel sei. Welche metacyklische Function dabei zu Grunde gelegt wird, ist theoretisch ganz gleichgültig; praktisch dagegen kann durch geschickte Wahl die Rechnung, welche auf die Gleichung der gewählten metacyklischen Function führt, erheblich abgekürzt werden*).

Es seien $z_0,\ z_1,\ z_2,\ z_3,\ z_4$, oder kurz $0, 1, 2, 3, 4$ die fünf Wurzeln einer Gleichung fünften Grades. Wir betrachten die Function der Wurzeln

(1) $$y_1 = 0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 0.$$

Um die zugehörige Gruppe G zu finden, suchen wir zunächst alle Substitutionen, die 0 in a umwandeln, wobei $a = 1,\ 2,\ 3,\ 4$ sein kann. Es folgt zunächst, dass 1 in $a - 1$ oder in $a + 1$ übergeht. Im zweiten Falle hat man sofort die Substitution

$$s_a = (0,\ a,\ 2a,\ 3a,\ 4a) \pmod{5},$$

d. h. alle Potenzen von

$$s_1 = (0,\ 1,\ 2,\ 3,\ 4).$$

Im zweiten Falle ergiebt sich die Substitution

$$t = \begin{pmatrix} 0, & 1 & , & 2 & , & 3 & , & 4 \\ a, & a-1 & , & a-2 & , & a+2 & , & a+1 \end{pmatrix} \pmod{5},$$

bei welcher für jedes a ein Element ungeändert bleibt, nämlich das durch $3a$ charakterisirte.

*) Vgl. hierzu C. Runge, Acta math. 7 (1885), p. 173 und D. Sélivanoff, Bull. soc. math. 21 (1893), p. 97.

Hieraus folgt schon, da allein die Potenzen von s_1 sämmtliche Elemente umsetzen, dass G nur noch Substitutionen enthält, welche ein Element oder alle Elemente in Ruhe lassen (§ 572). Diejenigen, welche 0 nicht umsetzen, sind, wie (1) zeigt,

$$s_0 = 1 \quad \text{und} \quad t_0 = (14)(23).$$

G hat also die Ordnung 10; es ist die halbmetacyklische Gruppe § 536; sie ist ein Theiler der alternirenden Gruppe. Die Function y_1 hat zwölf Werthe, die wir folgendermassen schreiben wollen

$$\begin{array}{ll}
y_1 = 0\cdot1+1\cdot2+2\cdot3+3\cdot4+4\cdot0, & y_7 = 0\cdot2+2\cdot4+4\cdot1+1\cdot3+3\cdot0;\\
y_2 = 0\cdot2+2\cdot4+4\cdot3+3\cdot1+1\cdot0, & y_8 = 0\cdot1+1\cdot2+2\cdot4+4\cdot3+3\cdot0;\\
y_3 = 0\cdot2+2\cdot1+1\cdot4+4\cdot3+3\cdot0, & y_9 = 0\cdot1+1\cdot3+3\cdot2+2\cdot4+4\cdot0;\\
y_4 = 0\cdot1+1\cdot4+4\cdot2+2\cdot3+3\cdot0, & y_{10} = 0\cdot2+2\cdot3+3\cdot4+4\cdot1+1\cdot0;\\
y_5 = 0\cdot1+1\cdot3+3\cdot4+4\cdot2+2\cdot0, & y_{11} = 0\cdot2+2\cdot1+1\cdot3+3\cdot4+4\cdot0;\\
y_6 = 0\cdot2+2\cdot3+3\cdot1+1\cdot4+4\cdot0, & y_{12} = 0\cdot1+1\cdot4+4\cdot3+3\cdot2+2\cdot0.
\end{array}$$

Die zugehörigen Gruppen für diese einzelnen Functionen wollen wir mit

$$G_1 = G,\ G_2,\ \cdots\ G_6;\ G_7,\ G_8,\ \cdots\ G_{12}$$

bezeichnen; sie werden gefunden, wenn man $G = G_1$ durch passende Substitutionen $\sigma_1 = 1,\ \sigma_2,\ \sigma_3, \cdots \sigma_6;\ \tau,\ \sigma_2\tau,\ \sigma_3\tau, \cdots \sigma_6\tau$ transformirt. Dabei sei

$$\begin{array}{lll}
\sigma_1 = 1 \quad ; & \sigma_2 = (1,2,4); & \sigma_3 = (1,2)(3,4);\\
\sigma_4 = (2,4,3); & \sigma_5 = (2,3,4); & \sigma_6 = (1,2,3) \quad ;
\end{array}$$
$$\tau = |\, h \quad 2h \,| = (1,2,4,3);$$

es gehören also $\sigma_1, \sigma_2, \cdots \sigma_6$ der alternirenden Gruppe an, während die Substitution τ keine gerade Substitution ist. Hierbei zeigt sich ferner

$$G_7 = \tau^{-1}G_1\tau = G_1,\quad G_8 = \tau^{-1}G_2\tau = G_2,\ \cdots\ G_{12} = \tau^{-1}G_6\tau = G_6;$$

es gehören also alle G_μ und $G_{\mu+6}$ zur gleichen Gruppe.

Da $\tau^2 = t_0$ ist, so wandelt jede Substitution, die ein y_μ in $y_{\mu+6}$ überführt, auch umgekehrt $y_{\mu+6}$ in y_μ um. Demgemäss hat $y_1 - y_7$ gleichfalls zwölf Werthe

$$\begin{array}{llll}
y_1 - y_7, & y_2 - y_8, & \cdots & y_6 - y_{12},\\
y_7 - y_1, & y_8 - y_2, & \cdots & y_{12} - y_6,
\end{array}$$

die wir mit $\varphi_1, \varphi_2, \cdots \varphi_6;\ -\varphi_1,\ -\varphi_2, \cdots -\varphi_6$ bezeichnen. Das Quadrat von $y_1 - y_7$ hat sechs Werthe, nämlich

$$\varphi_1 = (y_1 - y_7)^2,\quad \varphi_2 = (y_2 - y_8)^2,\quad \cdots\quad \varphi_6 = (y_6 - y_{12})^2.$$

Die zu φ_1 gehörige Gruppe wird durch die Substitutionen s_1, τ und ihre Combinationen gebildet; ihre Ordnung ist 20; es ist die metacyklische Gruppe und φ_1 ist eine metacyklische Function.

Es handelt sich nun um die Berechnung der Gleichung

$$(2) \qquad \prod_{\lambda=1}^{6}(\varphi-\varphi_\lambda) = \varphi^6 + a_1\varphi^5 + a_2\varphi^4 + \cdots + a_5\varphi + a_6 = 0,$$

welche $\varphi_1, \cdots \varphi_6$ als Wurzeln hat. Hierin sind $a_1, a_2, a_3, \cdots a_6$ symmetrische Functionen von $\varphi_1, \varphi_2, \cdots \varphi_6$. Alle Substitutionen der alternirenden Gruppe vertauschen diese Werthe nur unter sich; folglich sind $a_1, a_2, \cdots$ alternirend oder symmetrisch. Ferner gehen die homogenen Functionen ungeraden Grades a_1, a_3, a_5 in den φ bei einer Substitution, die nicht zur alternirenden Gruppe gehört, in $-a_1, -a_3, -a_5$ über, während die homogenen Functionen geraden Grades a_2, a_4, a_6 dabei ungeändert bleiben. Also sind a_1, a_3, a_5 alternirend; a_2, a_4, a_6 symmetrisch.

Demnach haben a_1, a_3, a_5 die Form $m_1\sqrt{\varDelta}, m_3\sqrt{\varDelta}, m_5\sqrt{\varDelta}$, wobei $\varDelta$ die Discriminante der Gleichung fünften Grades, und m_1, m_3, m_5 symmetrische ganze Functionen bedeuten. In z_0, z_1, z_2, z_3, z_4 sind $a_1, a_3, a_5, \sqrt{\varDelta}$ von den Dimensionen 2, 6, 10, 10; es müssen somit $m_1 = m_3 = 0$ sein, und m_5 wird eine Constante, die wir mit m bezeichnen. (2) geht daher in

$$(3) \qquad \varphi^6 + a_2\varphi^4 + a_4\varphi^2 + a_6 + m\sqrt{\varDelta}\varphi = 0$$

über.

§ 638. Die Berechnung der noch unbekannten Grössen gestaltet sich besonders einfach, falls man der Gleichung fünften Grades die Form

$$(4) \qquad f(z) = z^5 + uz + v = 0$$

ertheilt. In dieser sind u und v homogene Functionen der z_α von den Dimensionen 4 und 5, und da a_2, a_4, a_6 die Dimensionen 4, 8, 12 besitzen, so muss

$$a_2 = m_2 u, \quad a_4 = m_4 u^2, \quad a_6 = m_6 u^3$$

sein, wo m_2, m_4, m_6 ganze Zahlen bedeuten.

Diese, sowie m kann man durch ein numerisches Beispiel finden. Runge, von dem diese Betrachtungen stammen, wählt als solches $u = -1, v = 0$ und findet $\varDelta = -4^4$,

$$z_0, z_1, z_2, z_3, z_4 = 0, i, i^2, i^3, i^4;$$

$$\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6 = -2i, -2i, -2i, -2i, 2+4i, -2+4i;$$

$$\varphi^6 - m_2\varphi^4 + m_4\varphi^2 - m_6 + 16im\varphi = (\varphi+2i)^4(\varphi^2 - 8i\varphi - 20)$$
$$= \varphi^6 + 20\varphi^4 + 240\varphi^2 - 320 + 512i\varphi;$$

$$(\varphi^6 - m_2\varphi^4 + m_4\varphi^2 - m_6)^2 + 16^2m^2\varphi^2 = (\varphi^2+4)^4(\varphi^4 + 24\varphi^2 + 400).$$

Mithin wird die Gleichung für φ, nachdem man durch Quadrirung die Wurzel $\sqrt{\Delta}$ fortgeschafft hat,

(5) $$(\varphi^6 - 20u\varphi^4 + 240u^2\varphi^2 + 320u^3)^2 = 4^5\Delta\varphi^2, \quad \Delta = 4^4u^5 + 5^5v^4,$$

oder

(6) $$(\varphi^2 - 4u)^4(\varphi^4 - 24u\varphi^2 + 400u^2) = 4^5 \cdot 5^5 \cdot v^4\varphi^2.$$

Setzen wir $\varphi^2 = 4\psi$, so ist auch ψ eine metacyklische Function. Sie genügt der Gleichung

(5ᵃ) $$(\psi^3 - 5u\psi^2 + 15u^2\psi + 5u^3)^2 = \Delta\psi,$$

der man auch die Form geben kann

(6ᵃ) $$(\psi - u)^4(\psi^2 - 6u\psi + 25u^2) = 5^5v^4\psi.$$

§ 639. Nur wenn (5ᵃ) bezw. (6ᵃ) eine rationale Wurzel besitzt, ist

(4) $$f(z) \equiv z^5 + uz + v = 0$$

auflösbar, und stets dann. Denn wenn f reductibel ist, versteht sich dies von selbst; und wenn f irreductibel ist, dann ist ihre Gruppe metacyklisch oder steht unter der metacyklischen Gruppe, so dass also jedenfalls eine metacyklische Function der Wurzeln dem Rationalitätsbereiche angehört.

Dividirt man beide Seiten von (6ᵃ) durch u^6 und setzt $\psi = u \cdot \psi'$, $v = uv'$, so ergiebt sich

$$(\psi' - 1)^4(\psi'^2 - 6\psi' + 25) = 5^5\frac{v'^4\psi'}{u}$$

oder

(7) $$u = \frac{5^5v'^4\psi'}{(\psi' - 1)^4(\psi'^2 - 6\psi' + 25)}.$$

Sind nun ψ; u, v rationale Grössen, die (6ᵃ) befriedigen, so sind ψ'; u, v' rationale Grössen, die (7) befriedigen und umgekehrt; wählt man daher v', ψ' beliebig und u gemäss (7), dann liefern u, v eine auflösbare Gleichung (4); und umgekehrt, wenn (4) auflösbar ist, dann gehört zu rationalen Werthen von ψ'; v' das durch (7) bestimmte u.

Der Ausdruck (7) vereinfacht sich noch etwas, wenn man eine Substitution

$$\lambda = \frac{\psi' - 3}{4}, \quad \mu = \frac{5v'}{2(\psi' - 1)}$$

oder auch

$$\lambda = \frac{\psi - 3u}{4u}, \quad \mu = \frac{5v}{2(\psi - u)}$$

vornimmt. Dadurch wird

(8) $$u = \frac{5\mu^4(4\lambda + 3)}{\lambda^2 + 1}, \quad v = \frac{4\mu^5(2\lambda + 1)(4\lambda + 3)}{\lambda^2 + 1}, \quad \psi = \frac{5\mu^4(4\lambda + 3)^2}{\lambda + 1}.$$

Wir haben also bewiesen: Giebt man λ und μ irgend zwei Werthe irgend eines Rationalitätsbereiches, so ist die Form

$$z^5 + \frac{5\mu^4(4\lambda+3)}{\lambda^2+1}z + \frac{4\mu^5(2\lambda+1)(4\lambda+3)}{\lambda^2+1} = 0 \tag{9}$$

charakteristisch für auflösbare Gleichungen der Form

$$z^5 + uz + v = 0.$$

Von Glashan und P. Young*) stammt eine andere Form, nämlich

$$z^5 + \frac{5\mu_1^4(3-4\lambda_1)}{\lambda_1^2+1}z + \frac{4\mu_1^5(11-2\lambda_1)}{\lambda_1^2+1} = 0 \tag{10}$$

und von Bougaieff und Lachtine**) die folgende

$$z^5 + \frac{\mu_2^4(\lambda_2-1)(\lambda_2-11)}{4(\lambda_2^2+4)}z + \frac{\mu_2^5(\lambda_2-11)}{2(\lambda_2^2+4)} = 0. \tag{11}$$

Es gehen, wie bemerkt werden mag, (10) und (11) aus (9) hervor durch die Annahmen

$$\lambda_1 = \frac{4-3\lambda}{4\lambda+3}, \qquad \mu_1 = \mu;$$

bezw.

$$\lambda_2 = \frac{2(\lambda-2)}{2\lambda+1}, \qquad \mu_2 = -2\mu.$$

§ 640. An die Form

$$(\psi-u)^4(\psi^2-6u\psi+25u^2) - 5^5v^4\psi = 0 \tag{6a}$$

der Resolvente knüpft Sélivanoff folgende Bemerkung (l. c.).

Ist $u = \pm 1$, so entsteht

$$(\psi \mp 1)^4((\psi \mp 3)^2+16) - 5^5v^4\psi = 0, \tag{12}$$

woraus man ersieht, dass eine etwa vorhandene rationale Wurzel ψ positiv sein muss. Ist ferner v eine ganze Zahl, so kann nach § 241 ein solches rationales ψ auch nur ganz sein; da endlich in (6^a) das absolute Glied für $u = \pm 1$ gleich 25 wird, so kann ein rationales ψ nur ein Theiler von 25, d. h. gleich 1, 5 oder 25 werden. In keinem dieser drei Fälle tritt aber für v^4 eine vollständige vierte Potenz heraus. Sonach giebt es keine rationale Lösung für (6^a) bei $u = \pm 1$; d. h. die auflösbaren Gleichungen

$$z^5 \pm z + v = 0,$$

in denen v eine ganze Zahl bedeutet, sind reductibel.

*) Amer. Journ. of math. 7 (1885), p. 178, p. 170.

**) Moskau. Math. Samml. 15 (1890), p. 83.

Diese Sélivanoff'sche Methode lässt sich leicht verallgemeinern. Zuerst sehen wir aus (6^a) direct, dass ψ auch im allgemeinen Falle eine positive, ganze Zahl sein muss, wenn u, v ganz sind, und dass ψ ein Theiler von $25u^6$ wird. Weiter folgt aus derselben Gleichung, dass

$$\frac{\psi^2 - 6u\psi + u^2}{5\psi} = \varpi$$

eine vollständige vierte Potenz ist.

Ist u nicht durch 5 theilbar, so wird ψ als Theiler von $25u^6$ gleich $5^\alpha \tau$ ($\alpha = 0, 1, 2$), wobei τ nicht mehr durch 5 theilbar ist; in

$$\varpi = \frac{5^\alpha \tau^2 - 6u\tau + 5^{2-\alpha}u^2}{5\tau} \qquad (\tau \text{ nicht} \equiv 0 \text{ mod. } 5)$$

muss die 5 des Nenners sich wegheben, wenn ϖ eine vierte Potenz sein soll; und dies ist nur für $\alpha = 0$ oder $\alpha = 2$ möglich. Man hat dafür in diesen beiden Fällen

$$\varpi = \frac{\tau(\tau - u) - 5u\tau + 25u^2}{5\tau} \quad \text{oder} \quad \varpi = \frac{25\tau^2 - 5u\tau + u(u - \tau)}{5\tau}.$$

Es ist also in beiden Fällen τ ein Theiler von u^6, der mod. 5 zu u congruent ist. Ist nun u eine von 5 verschiedene Primzahl, so hat u^6 als Theiler $1, u, \cdots, u^6$. Man erkennt sofort, dass nur für ein $u \equiv \pm 1$ (mod. 5) ein solcher Theiler u^α congruent u werden kann, ausser wenn $\tau = u$ ist. In diesem Falle wird $\psi = 25u$ und $\varpi = 4u$; das ist aber bei unserer Annahme keine vierte Potenz. Also folgt, dass (6^a) keine rationale Wurzel liefert, wenn $u \equiv \pm 2$ (mod. 5) ist.

Ist ferner $u = 5$, so kann nur $\psi = 5^\alpha$ mit $\alpha = 0, 1, 2, \cdots 8$ sein. Dafür wird aber

$$\varpi = -6 + \frac{5^{2\alpha} + 5^2}{5^{\alpha+1}};$$

dies liefert, wenn der Bruch auf seine kleinste Benennung gebracht ist, für keins der α einen Nenner, welcher eine vierte Potenz wäre, folglich ist auch hier eine rationale Lösung von (6^a) unmöglich.

So haben wir gezeigt: Alle auflösbaren Gleichungen der Form

$$z^5 + uz + v = 0,$$

in denen u eine Primzahl und v eine ganze Zahl bedeutet, sind reductibel, falls u nicht $\equiv \pm 1$ (mod. 5) ist.

§ 641. Mc. Clintock*) behandelt eine andere metacyklische Resolvente und berechnet ihre Gleichung. Er setzt die halbmetacyklischen Functionen an:

*) Amer. Journ. of math. 8 (1886), p. 45; ib. 20 (1898), p. 157.

$$Y_1 = 0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 0 + 4 \cdot 0 \cdot 1,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Y_7 = 0 \cdot 2 \cdot 4 + 2 \cdot 4 \cdot 1 + 4 \cdot 1 \cdot 3 + 1 \cdot 3 \cdot 0 + 3 \cdot 0 \cdot 2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

Von diesen $Y_1, Y_2, \cdots Y_{12}$ gilt Aehnliches, wie von den $y_1, y_2, \cdots y_{12}$. Weiter sei

$$\Phi_1 = Y_1 - Y_7, \quad \Phi_2 = Y_2 - Y_8, \quad \cdots \quad \Phi_6 = Y_6 - Y_{12};$$

dann ist

$$t = \frac{Y_1 - Y_7}{y_1 - y_7} \tag{13}$$

seine metacyklische Resolvente.

Für diese findet er unter der Voraussetzung der Gleichung fünften Grades

$$f(z) = z^5 + 10 c_2 z^3 + 10 c_3 z^2 + 5 c_4 z + c_5 = 0 \tag{14}$$

die Resolventengleichung sechsten Grades

$$f(t) \cdot (l_0 t + l_1) - 25 (\gamma_0 t^3 + \gamma_1 t^2 + \gamma_2 t + \gamma_3) = 0, \tag{15}$$

wobei die Constanten folgende Bedeutung haben

$$\begin{aligned}
\gamma_0 &= -c_2^3 + c_2 c_4 - c_3^2, \\
\gamma_1 &= -c_2^2 c_3 + c_2 c_5 - c_3 c_4, \\
\gamma_2 &= -c_2 c_3^2 + c_2^2 c_4 + c_3 c_5 - c_4^2, \\
\gamma_3 &= 2 c_2 c_3 c_4 - c_2^2 c_5 - c_3^3;
\end{aligned}$$

$$\begin{aligned}
l_0 = {} & -15 c_2^4 c_4 + 10 c_2^3 c_3^2 - 2 c_2^2 c_3 c_5 + 14 c_2^2 c_4^2 - 22 c_2 c_3^2 c_4 + c_2 c_5^2 + 9 c_3^4 \\
& - 2 c_3 c_4 c_5 + c_4^3, \\
l_1 = {} & 9 c_2^4 c_5 - 20 c_2^3 c_3 c_4 + 10 c_2^2 c_3^3 + 8 c_2^2 c_4 c_5 - 12 c_2 c_3 c_4^2 - 2 c_2 c_3^2 c_5 \\
& + 6 c_3^3 c_4 + c_3 c_5^2 - c_4^3 c_5.
\end{aligned}$$

Hat (15) eine rationale Wurzel, dann ist (14) auflösbar. Mc. Clintock giebt nun in der citirten Arbeit mit Hülfe von drei Parametern und von t die Ausdrücke für c_2, c_3, c_4, c_5, für welche eine irreductible Gleichung (14) lösbar wird.

Achtundsechzigste Vorlesung.

Die allgemeinen Gleichungen fünften Grades.

§ 642. Bei Gelegenheit der Transformation von Gleichungen haben wir die allgemeinen Gleichungen fünften Grades auf eine beliebige der vier Bring-Jerrard'schen Formen (§ 116; Bd. I) reducirt*)

$$(1)\qquad \begin{array}{ll} \Phi^5 + \Phi - D = 0, & \Phi^5 - \Phi^2 - D = 0, \\ \Phi^5 + \Phi^3 - D = 0, & \Phi^5 - \Phi^4 - D = 0. \end{array}$$

Wir betrachten jetzt noch einmal eingehender die Transformationstheorie für die Gleichung

$$(2)\qquad f(x) = x^5 + Ax^4 + Bx^3 + Cx^2 + Dx + E = 0,$$

indem wir zunächst den Untersuchungen von L. Kiepert**) folgen.

Setzen wir die Tschirnhausen-Transformation an, in welcher u und v noch unbestimmte Grössen bedeuten,

$$(3)\qquad y = x^2 - ux + v,$$

so können wir in der Gleichung für y durch passende Wahl von u und v die Glieder mit y^4 und y^3 zum Verschwinden bringen. Dazu ist es nöthig, die beiden Gleichungen zweiten und ersten Grades

$$(4)\qquad \begin{array}{l} (2A^2 - 5B)u^2 + (4A^3 - 13AB + 15C)u \\ \qquad + (2A^4 - 8A^2B + 10AC + 3B^2 - 10D) = 0, \end{array}$$

$$(5)\qquad 5v = -Au - A^2 + 2B$$

zu befriedigen.

Bezeichnet man dann

$$\begin{array}{l} 5l = -C(u^3 + Au^2 + Bu + C) + D(4u^3 + 3Au + 2B) \\ \qquad - E(5u + 2A) - 10v^3, \end{array}$$

$$(6)\qquad \begin{array}{l} 5m = -D(u^4 + Au^3 + Bu^2 + Cu + D) + E(5u^3 + 4Au^2 + 3Bu + 2C) \\ \qquad + 5v^4 + 10lv, \end{array}$$

$$n = -E(u^5 + Au^4 + Bu^3 + Cu^2 + Du + E) - v^5 - 5lv^2 + 5mv,$$

so ergiebt sich die transformirte Gleichung in y

$$(7)\qquad y^5 + 5ly^2 - 5my + n = 0.$$

*) E. S. Bring hat diese Form zuerst aufgestellt; vgl. Harley, Quart. Journ. of math. 6 (1864); weiter Arch. f. Math. 41 (1864), p. 105; Klein, Ikosaeder, p. 143.

**) L. Kiepert, Auflösung der Gleichungen fünften Grades. Journ. f. Math. 87 (1879), p. 114.

Hierbei ist aber zu bemerken, dass y keine Resolvente in dem bisher von uns gebrauchten Sinne ist. Denn als Resolvente bezeichneten wir eine rationale Function der Wurzeln der vorgelegten Gleichung mit Coefficienten, die dem ursprünglichen oder einem erweiterten Rationalitätsgebiete angehören. Hier aber sind u und v nur dann rational, wenn die Discriminante der quadratischen Gleichung (4), nämlich der Ausdruck

$$5(8A^3C - 3A^2B^2 + 16A^2D - 38ABC + 12B^3 - 40BD + 45C^2)$$

ein vollständiges Quadrat wird. Dies findet also bei allgemeinen Gleichungen (2) nicht statt.

Zur weiteren Umformung von (7) setzt Kiepert

$$y = -\frac{\alpha + \beta z}{3 + z^2} \tag{8}$$

und sucht α und β so zu bestimmen, dass die Gleichung für z die Form

$$z^5 + 10z^3 + 45z - g = 0 \tag{9}$$

annimmt und also nur einen einzigen Parameter g enthält. Bildet man die Eliminante von (9) und von (8)

$$yz^2 + \beta z + (3y + \alpha) = 0$$

nach z in der Gestalt einer Determinante siebenter Ordnung, so erhält man als Gleichung für y ohne grosse Mühe

$$\begin{aligned} (1728 + g^2)y^5 + 5(8\alpha^3 - 72\alpha\beta^2 + g(\alpha^2\beta - \beta^3))y^2 \\ - 5(\alpha^4 + 18\alpha^2\beta^2 - 27\beta^4 + g\alpha\beta^3)y \\ + (\alpha^5 + 10\alpha^3\beta^2 + 45\alpha\beta^4 + g\beta^5) = 0; \end{aligned} \tag{7a}$$

diese wird mit (7) identisch, wenn man die drei Grössen α, β, g den drei Gleichungen entsprechend wählt:

$$\begin{aligned} 8\alpha^3 - 72\alpha\beta^2 + g\cdot(\alpha^2\beta - \beta^3) &= (1728 + g^2)l\ , \\ \alpha^4 + 18\alpha^2\beta^2 - 27\beta^4 + g\cdot(\alpha\beta^3) &= (1728 + g^2)m\,, \\ \alpha^5 + 10\alpha^3\beta^2 + 45\alpha\beta^4 + g\cdot(\beta^5) &= (1728 + g^2)n\ . \end{aligned} \tag{10}$$

Aus diesen erhält man sofort durch lineare Combinationen die beiden einfachen Relationen

$$l\beta^2 = m\alpha - n; \tag{11}$$

$$(\alpha^2 + 3\beta^2)^3 = (1728 + g^2)(n\alpha - m\beta^2). \tag{12}$$

Eliminirt man jetzt aus den beiden, in g quadratischen ersten Gleichungen von (10) diese Grösse g und führt durch (11) noch für

β die Unbekannte α ein, so entsteht eine Eliminante zehnten Grades, welche sich folgendermassen in Factoren zerlegen lässt:

$$R \equiv (m\alpha - n)^2 (l\alpha^2 + 3m\alpha - 3n)^3 \cdot [(l^4 - lmn + m^3)\alpha^2 + (11l^3m + ln^2 - 2m^2n)\alpha + (-27l^3n + 64l^2m^2 + mn^2)].$$

Der erste Factor liefert zunächst die Resultate

$$\alpha = \frac{n}{m}, \quad \beta = 0$$

und dann durch Einsetzung in die beiden ersten Gleichungen von (10) weiter

$$8m^2 = ln;$$

folglich ist dieser Fall bei der Behandlung allgemeiner Gleichungen (7) auszuschliessen und ebenso wegen der Relationen (6) bei allgemeinen Gleichungen (2).

Der zweite Factor der Eliminante liefert zunächst die Resultate

$$l\alpha^2 + 3m\alpha - 3n = 0,$$

$$\beta^2 = \frac{m\alpha - n}{l} = -\frac{\alpha^2}{3}.$$

Hierdurch gehen die drei Gleichungen (10) über in

$$8\alpha^3 + \frac{1}{3}g\alpha^2\beta = \frac{1}{4}(1728 + g^2)l \quad,$$

$$8\alpha^4 + \frac{1}{3}g\alpha^3\beta = -(1728 + g^2)m,$$

$$8\alpha^5 + \frac{1}{3}g\alpha^4\beta = 3(1728 + g^2)n \quad.$$

Da aber aus diesen eine Relation zwischen l, m, n, nämlich

$$3ln = 4m^2$$

folgt, so kann auch dies im allgemeinen Falle nicht eintreten.

Es bleibt also nur übrig*), zu setzen

$$(13) \qquad (l^4 - lmn + m^3)\alpha^2 + (11l^3m + ln^2 - 2m^2n)\alpha + (-27l^3n + 64l^2m^2 + mn^2) = 0.$$

Durch (11) und (12) gelangt man dann zu den Werthen für β und g. Die Formel (13) ergiebt

$$2(l^4 - lmn + m^3)\alpha = -(11l^3m + ln^2 - 2m^2n) \pm l\sqrt{\Delta'},$$

wobei*)

$$\Delta' = 108l^5n - 135l^4m^2 - 90l^2mn^2 + 320lm^3n - 256m^5 + n^4$$

---

*) In der Kiepert'schen Formel findet sich ein Druckfehler.

die Discriminante der Gleichung (7) ist. Demnach ist (8) in unserem Sinne eine eigentliche Resolvente von (7), indem die Coefficienten von (8) rational bekannt sind. Dass nämlich auch durch β keine neue Irrationalität eingeführt wird, zeigt Kiepert folgendermassen: Er erweitert (8) durch z^4+10z^2+45 und erhält dann für den Zähler wegen (9) den Ausdruck

$$\alpha(z^4+10z^2+45)+\beta(z^5+10z^3+45z)=\alpha(z^4+10z^2+45)+\beta g;$$

aus (10) und (11) folgt dann, dass βg eine rationale Function von α ist.

§ 643. Auf eine andere, höchst elegante Art liefert P. Gordan*) die Transformation von

$$f(x)\equiv x^5+Ax^4+Bx^3+Cx^2+Dx+E \tag{2}$$

auf die Form mit einem Parameter

$$z^5+10z^3+45z-g=0. \tag{9}$$

Gordan sucht zunächst eine Function der Wurzeln $x_1, x_2, \cdots x_5$ von (2), nämlich

$$\varphi(x)=x^2+\lambda x+\lambda_1, \tag{14}$$

welche den Bedingungen

$$\sum\varphi(x_\alpha)=0,\quad \sum\varphi^2(x_\alpha)=0 \qquad (\alpha=1,2,\cdots 5) \tag{14a}$$

unterworfen sein soll. Bezeichnen wir wie gewöhnlich die Summen der Wurzelpotenzen mit $s_1, s_2, \cdots$, so werden diese beiden Bedingungen zu

$$s_2+\lambda s_1+5\lambda_1=0,$$
$$s_4+2\lambda s_3+(\lambda^2+2\lambda_1)s_2+2\lambda\lambda_1 s_1+5\lambda_1^2=0;$$

aus diesen beiden numerischen Gleichungen lassen sich λ und λ_1 bestimmen.

Weiter werden zwei Functionen

$$\Theta(x)=x^3+\mu x+\mu_1,$$
$$\mathrm{H}(x)=x^4+\nu x+\nu_1$$

bestimmt, welche die Forderungen

$$\left.\begin{aligned}&\sum\Theta(x_\alpha)=0,\quad \sum\Theta(x_\alpha)\varphi(x_\alpha)=0,\\ &\sum\mathrm{H}(x_\alpha)=0,\quad \sum\mathrm{H}(x_\alpha)\varphi(x_\alpha)=0,\end{aligned}\right\}\quad(\alpha=1,2,\cdots 5)$$

oder auch, durch die s ausgedrückt,

$$s_3+\mu s_1+5\mu_1=0,$$
$$s_5+\lambda s_4+(\lambda_1+\mu)s_3+(\lambda\mu+\mu_1)s_2+(\lambda_1\mu+\lambda\mu_1)s_1+5\lambda_1\mu_1=0;$$

*) Math. Ann. 28 (1887), p. 152.

$$s_4 + \nu s_1 + 5\nu_1 = 0,$$
$$s_6 + \lambda s_5 + \lambda s_4 + \nu s_3 + (\lambda\nu + \nu_1)s_2 + (\lambda_1\nu + \lambda\nu_1)s_1 + 5\lambda_1\nu_1 = 0$$

befriedigen. Aus diesen vier linearen Gleichungen bestimmen sich die vier Grössen μ, μ_1; ν, ν_1 eindeutig.

Endlich setzen wir eine Function linear aus H und Θ zusammen

$$\psi(x) = \mathsf{H}(x) + \varrho\Theta(x),$$

wobei ϱ durch die Bedingung bestimmt werden soll, dass

$$\sum\psi^2(x_\alpha) = \varrho^2\sum\Theta^2(x_\alpha) + 2\varrho\sum\Theta(x_\alpha)\mathsf{H}(x_\alpha) + \sum\mathsf{H}^2(x_\alpha) = 0$$
$$(\alpha = 1, \cdots 5)$$

sei. Die Function ψ hat alsdann die Form

$$\psi(x) = x^4 + \varrho x^3 + \varrho_1 x + \varrho_2, \tag{15}$$

und sie erfüllt die drei Bedingungen

$$\sum\psi(x_\alpha) = 0, \quad \sum\psi^2(x_\alpha) = 0, \quad \sum\varphi(x_\alpha)\psi(x_\alpha) = 0 \tag{16}$$
$$(\alpha = 1, 2, \cdots 5).$$

Zwischen den beiden Functionen φ und ψ besteht eine für jedes x_α gültige quadratische Relation. Denn die neun Ausdrücke

$$\varphi(x_\alpha),\ \psi(x_\alpha),\ \varphi^2(x_\alpha),\ \varphi(x_\alpha)\psi(x_\alpha),\ \psi^2(x_\alpha),\ f(x_\alpha),$$
$$x_\alpha f(x_\alpha),\ x_\alpha^2 f(x_\alpha),\ x_\alpha^3 f(x_\alpha)$$

steigen in x_α höchstens bis zum achten Grade. Eliminirt man die acht Grössen x_α, x_α^2, $\cdots x_\alpha^8$ aus den neun in ihnen linearen Gleichungen

$$x_\alpha^2 + \lambda x_\alpha + \lambda_1 - \varphi(x_\alpha) = 0, \cdots; \quad x_\alpha^5 + Ax_\alpha^4 + \cdots = 0, \cdots$$

so wird die Resultante, welche man sofort in Determinantenform erhält,

$$\begin{aligned} c_{11}\varphi^2(x_\alpha) + 2c_{12}\varphi(x_\alpha)\psi(x_\alpha) + c_{22}\psi^2(x_\alpha) + c_1\varphi(x_\alpha) \\ + c_2\psi(x_\alpha) + c_0 = 0 \end{aligned} \tag{17}$$

die quadratische Relation liefern.

Summirt man nach $\alpha = 1, 2, \cdots 5$, so erkennt man wegen (16), dass $c_0 = 0$ ist.

Setzen wir nun an

$$\begin{aligned} h &= c_{11}\varphi + \left(c_{12} + \sqrt{c_{12}^2 - c_{11}c_{22}}\right)\psi, \\ h_1 &= c_{11}\varphi + \left(c_{12} - \sqrt{c_{12}^2 - c_{11}c_{22}}\right)\psi; \end{aligned} \tag{18}$$

$$d = \frac{c_1 c_{12} - c_{11}c_2}{\sqrt{c_{12}^2 - c_{11}c_{22}}} + c_1, \quad d_1 = \frac{c_1 c_{12} - c_{11}c_2}{\sqrt{c_{12}^2 - c_{11}c_{22}}} - c_1,$$

dann geht (17) in die kurze Form

$$2hh_1 = hd_1 - dh_1$$

über, und wir können eine Grösse y vermöge

(19) $$y = \frac{d}{h} + 1 = \frac{d_1}{h_1} - 1$$

als neue Variable einführen, für welche dann

(20) $$\frac{h}{d} = \frac{1}{y-1}, \quad \frac{h_1}{d_1} = \frac{1}{y+1}$$

wird.

Die transformirte Gleichung für y möge

(21) $$y^5 + \alpha_1 y^4 + \alpha_2 y^3 + \alpha_3 y^2 + \alpha_4 y + \alpha_5 \equiv F(y)$$

sein; es müssen zwischen ihren Coefficienten nothwendig Relationen stattfinden. Aus (18), (14^a) und (16) ergiebt sich

$$\sum h(x_\alpha) = 0, \quad \sum h^2(x_\alpha) = 0, \quad \sum h_1(x_\alpha) = 0, \quad \sum h_1^2(x_\alpha) = 0$$
$$(\alpha = 1, 2, \cdots 5),$$

und daher wegen (19)

$$\sum \frac{1}{y_\alpha - 1} = 0, \quad \sum \left(\frac{1}{y_\alpha - 1}\right)^2 = 0, \quad \sum \frac{1}{y_\alpha + 1} = 0,$$
$$\sum \left(\frac{1}{y_\alpha + 1}\right)^2 = 0.$$

Daraus folgt weiter, dass in den Gleichungen

$$F(y+1) = 0 \quad \text{und} \quad F(y-1) = 0$$

die Coefficienten des vorletzten und des drittletzten Gliedes verschwinden müssen. Das liefert mit Hülfe von (21) die Relationen

$$\begin{aligned}
10 + 6\alpha_1 + 3\alpha_2 + \alpha_3 \qquad &= 0, \\
5 + 4\alpha_1 + 3\alpha_2 + 2\alpha_3 + \alpha_4 &= 0, \\
-10 + 6\alpha_1 + 3\alpha_2 + \alpha_3 \qquad &= 0, \\
5 - 4\alpha_1 + 3\alpha_2 - 2\alpha_3 + \alpha_4 &= 0,
\end{aligned}$$

welche sich leicht zu

$$10 + 3\alpha_2 = 0, \quad 6\alpha_1 + \alpha_3 = 0,$$
$$5 + 3\alpha_2 + \alpha_4 = 0, \quad 4\alpha_1 + 2\alpha_3 = 0$$

vereinfachen lassen und die Resultate

$$\alpha_1 = \alpha_3 = 0, \quad \alpha_4 = 5, \quad \alpha_2 = -\frac{10}{3},$$

(22) $$F(y) \equiv y^5 - \frac{10}{3} y^3 + 5y + \alpha_5 = 0$$

ergeben. Setzt man endlich

$$y = \frac{z}{\sqrt{3}},$$

so entsteht als definitive Form

$$(9^a) \qquad z^5 - 10z^3 + 45z - g = 0.$$

Diese ist von (9) nur unwesentlich verschieden, da $z = \xi\sqrt{-1}$ die eine der beiden Formen in die andere überführt. (9) oder (9^a) heisst nach Brioschi*) die Brioschi'sche Resolvente.

Ist die Gleichung (22) aufgelöst, dann kann man aus ihren Wurzeln y_α diejenigen von (2) auf folgendem Wege herleiten.

Die Gleichungen (18) und (20) ergeben

$$(23) \qquad \varphi_\alpha = \frac{d\left(\sqrt{c_{12}^2 - c_{11}c_{22}} - c_{12}\right)}{2c_{11}\sqrt{c_{12}^2 - c_{11}c_{22}}(y_\alpha - 1)} + \frac{d_1\left(\sqrt{c_{12}^2 - c_{11}c_{22}} + c_{12}\right)}{2c_{11}\sqrt{c_{12}^2 - c_{11}c_{22}}(y_\alpha + 1)}$$

$$(\alpha = 1, 2, \cdots 5),$$

wobei φ_α den Werth von $\varphi(x)$ bedeuten soll, den diese Function annimmt, wenn man $y = y_\alpha$ setzt. Nun ist nach (14)

$$x^2 + \lambda x + \lambda_1 - \varphi = 0;$$

setzt man $\xi - \frac{\lambda}{2}$ für x und führt die Werthe $\xi_1, \xi_2, \cdots \xi_5$ entsprechend den Werthen $y_1, y_2, \cdots y_5$ ein, dann folgt

$$\xi_\alpha^2 = \varphi_\alpha + \frac{\lambda^2}{4} - \lambda_1.$$

Dieselbe Substitution wandelt (2) um in

$$\begin{aligned} 0 = \xi^5 &+ \xi^4\left(-\frac{5}{2}\lambda + A\right) + \xi^3\left(\frac{5}{2}\lambda^2 - 2\lambda A + B\right) \\ &+ \xi^2\left(-\frac{5}{4}\lambda^3 + \frac{3}{2}\lambda^2 A - \frac{3}{2}\lambda B + C\right) \\ &+ \xi\left(\frac{5}{16}\lambda^4 - \frac{1}{2}\lambda^3 A + \frac{3}{4}\lambda^2 B - \lambda C + D\right) \\ &+ \left(-\frac{1}{32}\lambda^5 + \frac{1}{16}\lambda^4 A - \frac{1}{8}\lambda^3 B + \frac{1}{4}\lambda^2 C - \frac{1}{2}\lambda D + E\right) \\ &= \xi\left[\xi^4 + A_2\xi^2 + A_4\right] + \left[A_1\xi^4 + A_3\xi^2 + A_5\right]. \end{aligned}$$

Ersetzt man die geraden Potenzen ξ^2, ξ^4 der letzten Zeile durch ihre Ausdrücke in den φ, so entsteht, wenn man von ξ_α auf $x_\alpha = \xi_\alpha - \frac{\lambda}{2}$ zurückgeht,

$$(24) \quad x_\alpha = -\frac{\lambda}{2} - \frac{A_1\left(\varphi_\alpha + \frac{1}{4}\lambda^2 - \lambda_1\right)^2 + A_3\left(\varphi_\alpha + \frac{1}{4}\lambda^2 - \lambda_1\right) + A_5}{\left(\varphi_\alpha + \frac{1}{4}\lambda^2 - \lambda_1\right)^2 + A_2\left(\varphi_\alpha + \frac{1}{4}\lambda^2 - \lambda_1\right) + A_4}.$$

Vermöge dieser Gleichung ergiebt sich zu jeder Wurzel von (22) oder von (9^a) eindeutig eine Wurzel der Gleichung (2) $f(x) = 0$.

---

*) Math. Ann. 13, p. 109—160.

§ 644. Wenn man, um eine neue Resolvente zu erlangen, in (9^a)

$$v = \frac{1}{z^2 - 3}$$

setzt und aus der hiermit identischen Gleichung $z^2 - \frac{3v+1}{v} = 0$ und (9^a) die Grösse z eliminirt, dann ergiebt sich durch einfache Determinantenausrechnung ohne Schwierigkeit

$$(25) \qquad (g^2 - 12^3)\,v^5 + 40v^2 - 5v + 1 = 0,$$

also eine Gleichung fünften Grades ohne vierte und ohne dritte Potenz der Unbekannten. F. Klein bezeichnet solche Gleichungen, bei denen die Summe der Wurzeln sowie die Summe der Wurzelquadrate Null ist, als Hauptgleichungen.

Eine andere derartige Hauptgleichung erhalten wir, wenn wir in (9^a)

$$w = \frac{u}{g\,(3 - u^2)}$$

substituiren und also aus (9^a) und aus

$$u^2 + \frac{1}{gw}u - 3 = 0$$

die Unbekannte u eliminiren. Man erhält dabei

$$(26) \qquad (g^2 - 1728)\,w^5 - 5\frac{1}{g^2}w^2 - 135\frac{1}{g^4}w - \frac{1}{g^4} = 0.$$

Die bisher betrachteten Gleichungen

$$(1) \qquad \varphi^5 + \varphi - D = 0; \qquad \text{(Bring-Jerrard)},$$

$$(9^a) \qquad z^5 - 10z^3 + 45z - g = 0; \qquad \text{(Brioschi)},$$

$$(25) \qquad (g^2 - 12^3)\,v^5 + 40v^2 - 5v + 1 = 0; \qquad \text{(Klein-Gordan)},$$

$$(26) \qquad (g^2 - 12^3)\,w^5 - 5\cdot\frac{1}{g^2}w^2 - 135\cdot\frac{1}{g^4}w - \frac{1}{g^4} = 0 \qquad \text{„} \quad \text{„}$$

haben die wichtige Eigenthümlichkeit, je von nur einem einzigen Parameter abhängig zu sein. Wir haben bereits darauf aufmerksam gemacht, dass die Grössen φ, z, v nicht in unserem eigentlichen Sinne als Resolventen bezeichnet werden dürfen, da sie keine rationalen Functionen der Wurzeln von der vorgelegten Gleichung

$$(2) \qquad x^5 + Ax^4 + Bx^3 + Cx^2 + Dx + E = 0$$

sind. Die Grössen z und v fordern die Einführung einer Quadratwurzel, die Grösse φ überdies diejenige einer dritten Wurzel aus Functionen von x. Klein bezeichnet diese Irrationalitäten als accessorische.

Unsere früheren Untersuchungen haben uns gezeigt, dass eine Auflösung von (2) durch Radicalzahlen unmöglich sei. Es fragt sich nun, in welcher Weise der Kreis der gestatteten Hülfsmittel erweitert werden muss, um von einer Lösung der Gleichungen fünften Grades reden zu dürfen. Ch. Hermite spricht sich hierüber (Paris, C. R. 46 (1858)) folgendermassen aus: „Diese Unmöglichkeit der Auflösung von Gleichungen fünften Grades weist auf die Nothwendigkeit hin, ein neues analytisches Element einzuführen“ (also z. B. die Wurzeln von (1) als bekannt anzunehmen). „Dabei muss man aber zusehen, ob die Einfachheit in der Form irgend welche Schlüsse über die Natur der Wurzeln zulässt. Für

$$z^3 - 3z + 2a = 0$$

genügt es z. B. $a = \sin\alpha$ zu setzen, um als die drei Wurzeln

$$z = 2\sin\frac{\alpha}{3},\quad 2\sin\frac{\alpha+2\pi}{3},\quad 2\sin\frac{\alpha+4\pi}{3}$$

zu finden.“

Der Hermite'schen Forderung wird, wie sich dann zeigt, durch Benutzung der elliptischen Functionen genüge geleistet. Wir wollen die nothwendigsten Formeln hierfür kurz zusammenstellen.

§ 645. Jacobi zeigt in dem Werke: „fundamenta nova theoriae functionum ellipticarum“, dass man den Differentialausdruck

$$\frac{dx}{\sqrt{(1-x^2)(1-\varkappa^2x^2)}}, \tag{27}$$

in welchem $\varkappa$ der Modul heisst, durch passend gewählte Substitutionen

$$y = \frac{U(x)}{V(x)} \tag{28}$$

mit ganzen Functionen U, V in einen Ausdruck ähnlicher Form

$$\frac{1}{M}\frac{dy}{\sqrt{(1-y^2)(1-\lambda^2y^2)}}, \tag{27^a}$$

in dem M constant ist und Multiplicator genannt wird, transformiren kann.

Die Transformation heisst von n^{ter} Ordnung, wenn $U(x)$ und $V(x)$ in (28) bis zum n^{ten} Grade in x aufsteigen. Für jedes n giebt es Transformationsformeln; wir beschränken uns auf ungerade Primzahlen n.

λ heisst der transformirte Modul. Zwischen

$$u = \sqrt[4]{\varkappa} \quad\text{und}\quad v = \sqrt[4]{\lambda}$$

besteht eine Gleichung vom Grade $(n+1)$ in u und v. Das ist die

sogenannte **Modulargleichung.** Diese lautet z. B. für $n = 3$

$$u^4 - v^4 + 2uv(1 - u^2v^2) = 0$$

und für $n = 5$

$$u^6 - v^6 + 5u^2v^2(u^2 - v^2) + 4uv(1 - u^4v^4) = 0. \tag{29}$$

Setzt man, wie gewöhnlich,

$$K = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-\varkappa^2x^2)}}, \quad K' = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-\varkappa'^2x^2)}}; \quad (\varkappa^2 + \varkappa'^2 = 1),$$

$$q = e^{-\pi\frac{K'}{K}} = e^{i\pi\omega}, \tag{30}$$

dann wird u. A.

$$u = \varphi(\omega) = \sqrt[4]{\varkappa} = \sqrt{2}\, q^{\frac{1}{8}} \frac{\sum q^{2m^2+m}}{\sum q^{m^2}} \qquad (m = -\infty, \cdots + \infty), \tag{31}$$

und man erhält alle Werthe von v, wenn man in (31) statt $q^{\frac{1}{8}}$ der Reihe nach

$$q^{\frac{n}{8}},\ q^{\frac{1}{8n}},\ \alpha q^{\frac{1}{8n}},\ \cdots\ \alpha^{n-1} q^{\frac{1}{8n}} \qquad \left(\alpha = e^{\frac{2i\pi}{n}}\right) \tag{32}$$

einträgt; oder auch, wenn man statt ω substituirt, wie man hieraus sofort unter Berücksichtigung von (30) erkennt,

$$n\omega,\ \frac{\omega}{n},\ \frac{\omega+16}{n},\ \cdots\ \frac{\omega + 16(n-1)}{n}. \tag{32^a}$$

Diese Werthe von v bezeichnen wir, den gemachten Substitutionen entsprechend, der Reihe nach durch

$$v_\infty,\ v_0,\ v_1,\ \cdots\ v_{n-1}. \tag{33}$$

Benutzen wir also die in (31) eingeführte Functionalbezeichnung φ, so folgt, dass für $\sqrt[4]{\varkappa} = \varphi(\omega)$ die $(n+1)$ Werthe von v durch

$$v_\infty = (-1)^{\frac{n^2-1}{8}} \cdot \varphi(n\omega), \quad v_0 = \varphi\left(\frac{\omega}{n}\right), \quad v_1 = \varphi\left(\frac{\omega+16}{n}\right), \quad \cdots$$

$$v_{n-1} = \varphi\left(\frac{\omega + 16(n-1)}{n}\right)$$

gegeben sind.

E. **Galois** hat die Gruppe der Modulargleichungen, denen $\sqrt{(-1)^{\frac{n-1}{2}} n}$ adjungirt worden ist, bestimmt (Oeuvres, éd. Picard 1897, p. 27). Jedes v_h wird durch sie in ein v_{h_1} übergeführt, wobei

$$h_1 = \frac{ah+b}{ch+d} \qquad (ad - bc \equiv 1 \pmod{p})$$

ist, und a, b, c, d alle möglichen mit der in der Klammer angegebenen Beschränkung verträglichen Werthe annehmen können. Nach früheren Festsetzungen lassen sich diese Substitutionen in der Form

(34) $$s = \left| h \quad \frac{ah+b}{ch+d} \right| \qquad (ad - bc \equiv 1 \pmod{p})$$

schreiben. Die Ordnung der Gruppe G der Modulargleichungen ist $r = \frac{1}{2} n(n^2 - 1)$. Galois bemerkte, dass für $n = 5; 7; 11$ die Gruppe G einen Theiler G_1 der Ordnung $r_1 = \frac{1}{2}(n^2 - 1)$ hat, so dass man also hierfür Resolventen mit n Werthen construiren kann.

Betti*) war der Erste, der einen Beweis dieser Galois'schen Sätze veröffentlichte. Hermite**) vervollständigte die Theorie durch die Angabe, wie jene n-werthige Resolvente gebildet werden könnte.

Der Theiler G_1 der Gruppe hat für $n = 5$ die Ordnung

$$r_1 = \frac{1}{2}(n^2 - 1) = 12;$$

er entsteht durch die Combination der drei Substitutionen

$$s_1 = | h \quad 4h |, \quad s_2 = \left| h \quad \frac{1}{h} \right|, \quad s_3 = \left| h \quad \frac{h-2}{h+2} \right|.$$

s_1, s_2 liefern eine Gruppe der Ordnung 4; s_3 ist von der Ordnung 3; und da

$$s_3^{-1} s_1 s_3 = s_2; \quad s_3^{-1} s_2 s_3 = s_1 s_2$$

wird, so geben s_1, s_2, s_3 die Gruppe G_1 der Ordnung 12. Aus ihr entsteht G durch Hinzunahme der cyklischen Substitution

$$s_4 = | h \quad h+1 |.$$

Jede zu G_1 gehörige Function der v_λ hängt von einer Gleichung fünften Grades ab. Hermite benutzt die Resolvente

(35) $$\begin{aligned} x_0 &= \left[\varphi(5\omega) + \varphi\left(\frac{\omega}{5}\right)\right]\left[\varphi\left(\frac{\omega+16}{5}\right) - \varphi\left(\frac{\omega+64}{5}\right)\right]\left[\varphi\left(\frac{\omega+32}{5}\right) - \varphi\left(\frac{\omega+48}{5}\right)\right] \\ &= \Phi(\omega) = (v_0 - v_\infty)(v_1 - v_4)(v_2 - v_3), \end{aligned}$$

wobei übereinstimmend mit den obigen Einführungen $\varphi(5\omega) = -v_\infty$ gesetzt ist. Man sieht sofort, dass (35) durch s_1, s_2, s_3 nicht geändert wird. Durch $s_4, s_4^2, \cdots$ erhält man der Reihe nach

$$\begin{aligned} x_1 &= \left[\varphi(5\omega) + \varphi\left(\frac{\omega+16}{5}\right)\right]\left[\varphi\left(\frac{\omega+32}{5}\right) - \varphi\left(\frac{\omega}{5}\right)\right]\left[\varphi\left(\frac{\omega+48}{5}\right) - \varphi\left(\frac{\omega+64}{5}\right)\right] \\ &= (v_1 - v_\infty)(v_2 - v_0)(v_3 - v_4), \\ x_2 &= \left[\varphi(5\omega) + \varphi\left(\frac{\omega+32}{5}\right)\right]\left[\varphi\left(\frac{\omega+48}{5}\right) - \varphi\left(\frac{\omega+16}{5}\right)\right]\left[\varphi\left(\frac{\omega+64}{5}\right) - \varphi\left(\frac{\omega}{5}\right)\right] \\ &= (v_2 - v_\infty)(v_3 - v_1)(v_4 - v_0), \end{aligned}$$

. . . .

*) Annali di scienze matematiche (Tortolini), 4 (1853).

**) Paris, C. R. 46 (1858), p. 508; vgl. auch ibid. p. 512 Anmerkg.

Hermite zeigt weiter, dass die fünf Grössen x_0, x_1, x_2, x_3, x_4 einer Gleichung fünften Grades mit $\sum x_\lambda = 0$, $\sum x_\lambda^2 = 0$, $\sum x_\lambda^3 = 0$ genügen

(36) $$x^5 - 2^4 \cdot 5^3 \cdot u^4 (1-u^8)^2 \cdot x - 2^6 \sqrt{5^5}\, u^3 (1-u^8)^2 (1+u^8) = 0.$$

Diese besitzt demnach die fünf Wurzeln

$$\Phi(\omega), \quad \Phi(\omega+16), \quad \Phi(\omega+32), \quad \Phi(\omega+48), \quad \Phi(\omega+64).$$

§ 646. An die Theorie der Transformation des Ausdruckes (27) in (27ᵃ), nämlich

$$\frac{dx}{\sqrt{(1-x^2)(1-\varkappa^2x^2)}} = \frac{dy}{M\sqrt{(1-y^2)(1-\lambda^2y^2)}},$$

knüpfen sich noch andere Gleichungen an.

Man kann den Multiplicator M rational durch $\varkappa$ und λ vermittels der Formel

$$M^2 = n\frac{\varkappa - \varkappa^3}{\lambda - \lambda^3}\frac{d\lambda}{d\varkappa}$$

ausdrücken. Eliminirt man hieraus und aus der Modulargleichung zwischen $\varkappa$ und λ diese letzte Grösse, so erhält man zwischen M und $\varkappa$ eine in beiden Grössen bis zum Grade $(n+1)$ aufsteigende algebraische Gleichung. Es ist dies eine Multiplicatorgleichung. Für die Beziehung zwischen $\varkappa$ und λM; $\lambda' M$; u. s. w. gilt Aehnliches; auch die hierbei entstehenden Gleichungen heissen Multiplicatorgleichungen.

Den verschiedenen Werthen $v_\infty, v_0, v_1, \cdots$ der Modulargleichung entsprechen die Wurzeln $M_\infty, M_0, M_1, \cdots$ der Multiplicatorgleichung. Jacobi*) hat hinsichtlich des Zusammenhanges dieser M unter einander ein Theorem entdeckt, welches er mit Recht als „un des plus importants dans la théorie algébrique de la transformation et de la division des fonctions elliptiques" erklärt. Er findet nämlich, dass man mit Hülfe von $\frac{n+1}{2}$ Grössen $A, A_1, A_2, \cdots A_{\frac{n-1}{2}}$ die M folgendermassen darstellen kann:

(37) $$\begin{gathered}\sqrt{M_\infty} = \sqrt{(-1)^{\frac{n-1}{2}} n} \cdot A, \\ \sqrt{M_\varrho} = A + \alpha^\varrho A_1 + \alpha^{4\varrho} A_2 + \cdots + \alpha^{\left(\frac{n-1}{2}\right)^2 \varrho} A_{\frac{n-1}{2}}; \\ (\alpha = 0, 1, \cdots n-1),\end{gathered}$$

wobei $\alpha = e^{\frac{2\pi i}{n}}$ zu setzen ist. Daraus ergiebt sich sofort, dass man die Hälfte der Werthe von $\sqrt{M}$ durch die andere Hälfte linear darstellen kann.

*) Werke I, p. 261.

Allgemein heissen Gleichungen $(n+1)^{\text{ten}}$ Grades mit $y=\sqrt{M_\infty}$, $\sqrt{M_0}, \cdots$, für welche Beziehungen (37) bestehen, für die also die Galois'schen Gruppen übereinstimmen, Jacobi'sche Gleichungen.

Berechnet man die Gleichung mit den Wurzeln $y=\sqrt{M_\infty}$, $\sqrt{M_0}, \cdots$ für $n=5$, so ergiebt sich

$$(38)\quad (y-a)^6-4a(y-a)^5+10b(y-a)^3-4c(y-a)+5b^2-4ac=0;$$

$$a=A^2+A_1A_2;\quad b=8A^4A_1A_2-2A^2A_1^2A_2^2+A_1^3A_2^3-A(A_1^5+A_2^5);$$

$$c=80A^6A_1^2A_2^2-40A^4A_1^3A_2^3+5A^2A_1^4A_2^4$$
$$-A(32A^4-20A^2A_1A_2+5A_1^2A_2^2)(A_1^5+A_2^5)$$
$$+\frac{1}{4}(A_1^5+A_2^5)^2.$$

Für $y=M$ erhält man die zugehörige Multiplicatorgleichung durch

$$a=1,\quad b=0,\quad c=-64\varkappa^2(1-\varkappa^2)$$

in der Form

$$(39)\quad (y-1)^6-4(y-1)^5+256\varkappa^2(1-\varkappa^2)(y-1)+256\varkappa^2(1-\varkappa^2)=0$$

oder, falls $y=1+z$ gesetzt wird,

$$(39^a)\qquad z^6-4z^5+256\varkappa^2(1-\varkappa^2)z+256\varkappa^2(1-\varkappa^2)=0.$$

Substituirt man hier an Stelle von z eine Grösse v vermittels

$$v=z^4-4z^3=(M-1)^3(M-5),$$

dann findet man die Gleichung sechsten Grades

$$v^6+10d^2v^3+(16d^3-d^4)v+5d^4=0,$$

wobei $d=256\varkappa^2\varkappa'^2$ zu setzen ist. Trägt man jetzt noch

$$v=d^{\frac{2}{3}}w,\quad w=\frac{(M-1)^3(M-5)}{(16\varkappa\varkappa')^{\frac{4}{3}}}$$

ein, so ergiebt sich die Form einer Hauptgleichung fünften Grades

$$(40)\qquad w^6+10w^3+\frac{16-d}{d^{\frac{1}{3}}}w+5=0;\qquad (d=256\varkappa^2\varkappa'^2).$$

Es wurde oben bereits erwähnt, dass im allgemeinen Falle $\frac{n+1}{2}$ lineare Relationen unter den Wurzeln bestehen. Diese sind bei $n=5$ für (38)

$$\sqrt{M_0}+\sqrt{M_1}+\sqrt{M_2}+\sqrt{M_3}+\sqrt{M_4}=\sqrt{5M_\infty},$$
$$(41)\quad \sqrt{M_0}+\alpha^2\sqrt{M_1}+\alpha^4\sqrt{M_2}+\alpha\sqrt{M_3}+\alpha^3\sqrt{M_4}=0,\qquad \left(\alpha=e^{\frac{2\pi i}{\omega}}\right)$$
$$\sqrt{M_0}+\alpha^3\sqrt{M_1}+\alpha\sqrt{M_2}+\alpha^4\sqrt{M_3}+\alpha^2\sqrt{M_4}=0.$$

Brioschi hat nun für $n = 5$ eine Erniedrigung der Jacobi'schen Gleichungen um eine Einheit durchgeführt*), genau wie Hermite für die Modulargleichungen. Er berechnet aus den sechs Gleichungen

$$(37^a) \qquad \sqrt{M_\infty} = \sqrt{5}A, \quad \sqrt{M_\lambda} = A + \alpha^\lambda A_1 + \alpha^{4\lambda} A_2$$

die Grössen

$$(42) \qquad \begin{aligned} t_0 &= \frac{1}{\sqrt[4]{5}} [(M_\infty - M_0)(M_2 - M_3)(M_4 - M_1)]^{\frac{1}{2}}, \\ t_1 &= \frac{1}{\sqrt[4]{5}} [(M_\infty - M_1)(M_3 - M_4)(M_0 - M_2)]^{\frac{1}{2}}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

und findet für

$$\begin{aligned} C_0 &= -A_1(4A^2 - A_1A_2), \quad & C_1 &= 2AA_1^2 - A_2^3, \\ C_3 &= A_2(4A^2 - A_1A_2), \quad & C_2 &= -(2AA_2^2 - A_1^3) \end{aligned}$$

die Relationen

$$t_\nu = \alpha^\nu C_0 + \alpha^{2\nu} C_1 + \alpha^{3\nu} C_2 + \alpha^{4\nu} C_3; \qquad (\nu = 0, 1, \cdots 4).$$

Die $t_0, t_1, \cdots t_4$ sind daher die Wurzeln einer Gleichung fünften Grades, deren Coefficienten rationale Functionen der Coefficienten der Jacobi'schen Gleichung und der vierten Wurzel aus ihrer Discriminante sind:

$$(43) \qquad t^5 + 10bt^3 + 5(9b^2 - 4ac)t - 8\sqrt{-h} = 0,$$

$$h = 27b^5 - c^3 - 25a^3b^4 + 40a^4b^2c + 20a^2bc^2 - 45ab^3c - 16a^5c^2.$$

Unter der Voraussetzung der durch die elliptischen Functionen gelieferten Gleichungen (39^a) und (40) entstehen hieraus die besonderen Formen

$$(43^a) \quad t^5 + 1280\varkappa^2(1 - \varkappa^2)t + 2048\varkappa^2(1 - \varkappa^2)(1 - 2\varkappa^2) = 0,$$

und für den zweiten Fall

$$(43^b) \qquad t^5 + 10t^3 + 45t - 8\left[\frac{(16\varkappa^2\varkappa'^2 - 1)^3}{4\varkappa^2\varkappa'^2} - 27\right]^{\frac{1}{2}} = 0.$$

§ 647. Jetzt gehen wir zu der Hermite'schen Auflösung der Gleichungen fünften Grades über. Hermite vergleicht seine Resolventenform (§ 645)

$$(36) \quad x^5 - 2^4 \cdot 5^3 \cdot u^4(1 - u^8)^2 x - 2^6\sqrt{5^5}\,u^3(1 - u^8)^2(1 + u^8) = 0$$

$$(u = \varphi(\omega))$$

*) Math. Ann. 13 (1878), p. 139 ff.

mit der Bring-Jerrard'schen Form einer allgemeinen Gleichung fünften Grades

$$(1^a) \qquad \Phi^5 - \Phi - D = 0.$$

Um zu dieser von der allgemeinen Gleichung aus zu gelangen, ist die Auflösung einer Gleichung dritten und einer solchen vierten Grades nothwendig (vgl. § 116, Bd. I).

Setzt man nun

$$x = 2 \cdot \sqrt[4]{5^3} \cdot u\sqrt{1-u^8} \cdot \Phi,$$

$$D = \frac{2}{\sqrt[4]{5^5}} \cdot \frac{1+u^8}{u^2\sqrt{1-u^8}},$$

so stimmt (36) mit (1^a) überein. Aus der letzten Gleichung für D folgt die Bestimmung von $u^4 = \varkappa$ durch eine Gleichung vierten Grades. Zur Vereinfachung bezeichnen wir

$$\frac{\sqrt[2]{5^5}D^2}{4} = A;$$

dann wird jene Gleichung vierten Grades

$$\varkappa^4 + A\varkappa^3 + 2\varkappa^2 - A\varkappa + 1 = 0.$$

Diese Gleichung lässt eine analytische Lösung in dem oben § 644 angeführten Hermite'schen Sinne zu. Für

$$\frac{1}{4A} = \sin\alpha$$

erhält man nämlich die Werthe

$$\varkappa = \operatorname{tang}\frac{\alpha}{4}, \quad \operatorname{tang}\frac{\alpha+2\pi}{4}, \quad \operatorname{tang}\frac{\pi-\alpha}{4}, \quad \operatorname{tang}\frac{3\pi-\alpha}{4}.$$

Wählen wir einen dieser vier Werthe und benutzen denselben zur Bestimmung von ω, dann ergeben sich als Wurzeln von (1^a) unter Benutzung der Bezeichnung (35)

$$\frac{1}{2\sqrt[4]{5^3}}\,\frac{\Phi(\omega)}{\varphi(\omega)\sqrt{1-\varphi^8(\omega)}}; \quad \frac{1}{2\sqrt[4]{5^3}}\,\frac{\Phi(\omega+16)}{\varphi(\omega)\sqrt{1-\varphi^8(\omega)}}; \quad \frac{1}{2\sqrt[4]{5^3}}\,\frac{\Phi(\omega+32)}{\varphi(\omega)\sqrt{1-\varphi^8(\omega)}};$$

$$\frac{1}{2\sqrt[4]{5^3}}\,\frac{\Phi(\omega+48)}{\varphi(\omega)\sqrt{1-\varphi^8(\omega)}}; \quad \frac{1}{2\sqrt[4]{5^3}}\,\frac{\Phi(\omega+64)}{\varphi(\omega)\sqrt{1-\varphi^8(\omega)}}.$$

Es ist leicht zu sehen, dass an die Resolvente (43^a) der Multiplicatorgleichung dieselben Betrachtungen angeknüpft werden können.

§ 648. Während so Hermite seine Auflösung der Gleichung fünften Grades dadurch bewirkt, dass er die Modulargleichung reducirt, knüpft Kronecker und nach ihm noch allgemeiner Brioschi die Lösung direct an die Jacobi'sche Multiplicatorgleichung, indem er eine Resolvente sechsten Grades der vorgelegten Gleichung fünften Grades mit jener identificirt.

Statt der symmetrischen Gruppe der fünf Wurzeln x_0, x_1, x_2, x_3, x_4 der Gleichungen fünftes Grades können wir die alternirende Gruppe zu Grunde legen, da die Adjungirung der Quadratwurzel aus der Discriminante ausreicht, um vom ersten auf den zweiten Fall zu kommen.

Die Substitutionen der alternirenden Gruppe der fünf x_h lassen sich durch folgende drei Substitutionen erzeugen

$$(44) \qquad |h \quad h+1|; \quad |h \quad 4h|; \quad |h \quad 3h^3| \qquad (\text{mod. } 5)$$
$$(h = 0, 1, 2, 3, 4).$$

Die beiden ersten geben eine Gruppe von der Ordnung 10. Stellt man alle 60 Substitutionen der alternirenden Gruppe in bekannter Weise in einer Tabelle derart zusammen, dass die erste Zeile aus jenen zehn Substitutionen besteht, dann können die anderen fünf Zeilen durch Hinzunahme je einer der fünf Substitutionen

$$(x_1 x_3)(x_2 x_4); \quad (x_0 x_1 x_4 x_3 x_2); \quad (x_0 x_2 x_1); \quad (x_0 x_3 x_4); \quad (x_0 x_4 x_1 x_2 x_3)$$

hergeleitet werden. Diese sind nun identisch mit

$$(45) \qquad |h \quad 3h^3|; \quad |h \quad 3h^3+1|; \quad |h \quad 3h^3+2|; \quad |h \quad 3h^3+3|; \quad |h \quad 3h^3+4|,$$

d. h. es sind Combinationen des ersten und des dritten Typus in (44).

Wir bilden jetzt eine allgemeine cyklische Function der x_h, welche durch

$$v = (0\ 1\ 2\ 3\ 4)$$

bezeichnet werden mag; diese bleibt für $|h \quad h+1|$ und die Potenzen dieser Substitution und auch nur dafür ungeändert. Es sei weiter

$$v' = (0\ 4\ 3\ 2\ 1)$$

das Resultat der Anwendung von $|h \quad 4h|$ auf v, und wir bezeichnen

$$u_\infty = v - v'.$$

Dann hat u_∞^2 sechs Werthe. Die einzelnen Substitutionen (45) mögen aus u_∞ Werthe hervorrufen, die wir der Reihe nach bezeichnen

$$u_0, \quad u_1, \quad u_2, \quad u_3, \quad u_4.$$

Die Gleichung, deren Wurzeln $u_0^2, u_1^2, \cdots u_4^2, u_\infty^2$ sind, hat demnach Coefficienten, die rational aus den Coefficienten von (2) und aus der Quadratwurzel der Discriminante zusammengesetzt sind.

Es lassen sich noch andere Gleichungen von interessanteren Eigenschaften construiren, wenn man die u passend mit einander verbindet.

Es gehen nämlich

durch	die Werthe	u_∞,	u_0,	u_1,	u_2,	u_3,	u_4
$\mid h \quad h+1 \mid$		u_∞,	u_1,	u_2,	u_3,	u_4,	u_0,
$\mid h \quad 4h \mid$	in	$-u_\infty$,	$-u_0$,	$-u_4$,	$-u_3$,	$-u_2$,	$-u_1$,
$\mid h \quad 3h^3 \mid$		u_0,	u_∞,	$-u_1$,	u_3,	u_2,	$-u_4$

über. Versteht man unter t eine willkürliche Constante, so überzeugt man sich sofort davon, dass die sechs Resolventen z_λ der x

$$
(46)\qquad
\begin{aligned}
z_\infty &= tu_\infty + u_0 + u_1 + u_2 + u_3 + u_4,\\
z_0 &= tu_0 + u_\infty - u_1 + u_3 + u_2 - u_4,\\
z_1 &= tu_1 + u_\infty - u_2 + u_4 + u_3 - u_0,\\
z_2 &= tu_2 + u_\infty - u_3 + u_0 + u_4 - u_1,\\
z_3 &= tu_3 + u_\infty - u_4 + u_1 + u_0 - u_2,\\
z_4 &= tu_4 + u_\infty - u_0 + u_2 + u_1 - u_3
\end{aligned}
$$

unter dem Einflusse von (44) dieselben Substitutionen der Indices erleiden, wie diejenigen der u in der vorigen Tabelle sind.

Die alternirende Gruppe der x führt daher die Resolventen

$$z_\infty^2,\ z_0^2,\ z_1^2,\ z_2^2,\ z_3^2,\ z_4^2$$

lediglich in einander über; sie sind demnach Wurzeln einer Gleichung sechsten Grades, deren Coefficienten rational aus denen der x-Gleichung und aus der Quadratwurzel aus deren Discriminante gebildet sind.

Aus (46) folgt, wenn $\alpha = e^{\frac{2\pi i}{5}}$ bedeutet,

$$
\begin{aligned}
&z_0 + z_1 + z_2 + z_3 + z_4 = 5u_\infty + t(u_0 + u_1 + u_2 + u_3 + u_4),\\
&z_0 + \alpha^2 z_1 + \alpha^4 z_2 + \alpha z_3 + \alpha^3 z_4\\
&\qquad = (u_0 + \alpha^2 u_1 + \alpha^4 u_2 + \alpha u_3 + \alpha^3 u_4)(t + \rho - \rho^2 - \rho^3 + \rho^4),\\
&z_0 + \alpha^3 z_1 + \alpha z_2 + \alpha^4 z_3 + \alpha^2 z_4\\
&\qquad = (u_0 + \alpha^3 u_1 + \alpha u_2 + \alpha^4 u_3 + \alpha^2 u_4)(t + \rho - \rho^2 - \rho^3 + \rho^4).
\end{aligned}
$$

Da nun aus der Annahme

$$t = -\rho + \rho^2 + \rho^3 - \rho^4$$

durch Quadriren folgt $t^2 = 5$, so zeigt sich, dass bei $t = \sqrt{5}$

$$
(47)\qquad
\begin{aligned}
&z_0 + z_1 + z_2 + z_3 + z_4 = \sqrt{5}\, z_\infty ,\\
&z_0 + \alpha^2 z_1 + \alpha^4 z_2 + \alpha\, z_3 + \alpha^3 z_4 = 0,\\
&z_0 + \alpha^3 z_1 + \alpha\, z_2 + \alpha^4 z_3 + \alpha^2 z_4 = 0
\end{aligned}
$$

wird. Die Gleichung in z

$$
(48)\qquad (z - z_\infty^2)(z - z_0^2)(z - z_1^2)\cdots(z - z_4^2) = 0
$$

ist also eine Jacobi'sche Gleichung (vgl. Formel (41)); sie hat demnach die Gestalt (38).

Bisher war die Wahl der cyklischen Function v, aus welcher u_∞ gebildet wurde, noch keiner Beschränkung unterworfen. Wir wollen die hierin liegende Freiheit zur Vereinfachung der Gleichung (38) benutzen.

Ist neben v auch noch w eine cyklische Function der Grössen z, die nur von v verschieden sein soll, so werden auch für sie $\zeta_\infty, \zeta_0, \cdots$ den $z_\infty, z_0, \cdots$ entsprechend gebildet werden können, und bei willkürlichem p wird

$$
(49)\qquad Z_\lambda = z_\lambda + p\zeta_\lambda \qquad (\lambda = 0, 1, \cdots 4;\ \infty)
$$

als lineare Function der z_λ und der ζ_λ den Gleichungen genügen, die (47) entsprechen. Es wird demgemäss

$$
(49^a)\qquad (Z - Z_\infty^2)(Z - Z_0^2)(Z - Z_1^2)\cdots(Z - Z_4^2) = 0
$$

gleichfalls eine Jacobi'sche Gleichung sein.

In ihr können wir die dem a in (38) entsprechende Grösse zu Null machen, wenn wir p durch die numerische quadratische Gleichung

$$
(50)\qquad p^2 \sum \zeta_\lambda^2 + 2p \sum z_\lambda \zeta_\lambda + \sum z_\lambda^2 = 0
$$

bestimmen. Dadurch geht (49^a) gemäss (38) in

$$
Z^6 + 10B \cdot Z^3 - 4C \cdot Z + 5B^2 = 0
$$

über und für $Z = B^{\frac{1}{3}} U$ in

$$
U^6 + 10U^3 - 4\frac{C}{B^{\frac{5}{3}}} U + 5 = 0.
$$

Vergleicht man diese Form mit der aus der Multiplicatorgleichung entspringenden Gleichung (40), so folgt, dass, wenn man $\varkappa^2$ aus

$$
\frac{(16 - d)^3}{d} = -64 \frac{C^3}{B^5}; \qquad d = 256\,\varkappa^2 \varkappa'^2
$$

berechnet, indem man zuerst d von der Lösung einer Gleichung dritten Grades abhängig macht, durch

$$Z = B^{\frac{1}{3}} \frac{(M-1)^3 (M-5)}{(16 \varkappa \varkappa')^{\frac{4}{3}}}$$

die Gleichung sechsten Grades in Z mit Hülfe von elliptischen Functionen aufgelöst wird.

Kennt man die sechs Werthe (49), so werden die Wurzeln x der vorgelegten Gleichung fünften Grades rational darstellbar, da ja die einzelnen Gruppen der Functionen (49) keine Substitutionen gemeinsam haben (§ 543 und § 579).

§ 649. Kronecker machte, wie schon oben erwähnt wurde, zuerst darauf aufmerksam, dass bei Gleichungen fünften Grades Resolventen mit Einem Parameter nicht bestehen. Den ersten Beweis dieses Satzes gab F. Klein auf Grund seiner Untersuchungen über das Ikosaeder*); einen einfacheren und directen lieferte später P. Gordan**). Der nun folgende Beweis schliesst sich dem Gordan'schen Gedankengange eng an.

Wir beginnen mit einem von J. Lüroth stammenden Satze***).

Es sei die Function

$$G(z, z') = g(z) g_1(z') - g_1(z) g(z') \tag{51}$$

gegeben; $g(u)$ und $g_1(u)$ seien hierin ganze Functionen ohne gemeinsamen Theiler. $G(z, z')$ sei in z vom Grade n. Die Gleichung

$$G(z, z') = 0 \tag{52}$$

in z hat keine vielfachen Wurzeln $z = \zeta$; denn sonst hätten die beiden Functionen

$$g(z) g_1(z') - g_1(z) g(z') = \gamma(z, z'),$$
$$g'(z) g_1(z') - g_1'(z) g(z') = \gamma_1(z, z')$$

einen gemeinsamen Theiler; den gleichen hätte dann ebenfalls

$$g_1'(z) \cdot \gamma(z, z') - g_1(z) \cdot \gamma_1(z, z') = g_1(z') \cdot [g(z) g_1'(z) - g'(z) g_1(z)]$$

und also auch

$$g(z) g_1'(z) - g'(z) g_1(z);$$

d. h. $G(z, z')$ wäre durch eine Function von z allein theilbar, und $g(z)$ hätte gegen die Annahme mit $g_1(z)$ einen Factor gemein.

Es ist ferner

$$G(z', z) = -G(z, z') \tag{53}$$

und deshalb ist $z = z'$ eine Wurzel von (52).

*) Vorlesungen üb. d. Ikosaeder (1884), p. 258.

**) Math. Ann. 29 (1887), p. 318.

***) Math. Ann. 9 (1876), p. 163.

Sind nun $z' = z_0', z_1', z_2', \cdots z_{n-1}'$ sämmtliche Wurzeln von (52), dann sind dieselben Grössen auch sämmtliche Wurzeln von

$$G(z, z_\alpha') = 0 \qquad (\alpha = 0, 1, \cdots n-1), \tag{52^a}$$

wie sich aus (51) ergiebt. Die gleichen Wurzeln hat jede Gleichung

$$G(z_\alpha', z) = 0. \tag{52^b}$$

Nun möge eine ganze Function

$$\Gamma(z, z')$$

vom n^{ten} Grade in z gegeben sein, deren Nullwerthe $z = z', z_1', \cdots z_{n-1}'$ sind, und die so beschaffen ist, dass alle Gleichungen in z

$$\Gamma(z, z_\alpha') = 0 \qquad (\alpha = 0, 1, \cdots n-1)$$

dieselben Wurzeln aufweisen. Wir wollen die Natur dieser Function Γ untersuchen. Es sei

$$\Gamma(z, z') = \varphi_0(z') \cdot z^n + \varphi_1(z') \cdot z^{n-1} + \cdots + \varphi_n(z'),$$

dann folgt aus den Annahmen für jeden Index $\varkappa = 1, 2, \cdots n$

$$\frac{\varphi_\varkappa(z_\alpha')}{\varphi_0(z_\alpha')} = \frac{\varphi_\varkappa(z_\beta')}{\varphi_0(z_\beta')} \qquad (\alpha, \beta = 0, 1, \cdots n-1),$$

so dass jede der Gleichungen

$$\varphi_0(z)\varphi_\varkappa(z') - \varphi_\varkappa(z)\varphi_0(z') = 0 \qquad (\varkappa = 1, 2, \cdots n) \tag{54}$$

dieselben Wurzeln hat wie $\Gamma(z, z') = 0$. Dabei können nicht alle Gleichungen (54) identisch erfüllt sein; die hingeschriebene möge zu den nicht identisch erfüllten gehören.

Gilt weiter

$$\Gamma(z, z') = \text{const.}\ \Gamma(z', z),$$

woraus durch Iteration der Vertauschung sofort const. $= \pm 1$ folgt, dann muss einer der Ausdrücke (54) zum n^{ten} Grade aufsteigen. Sind ferner die $z', z_1', \cdots z_{n-1}'$ unter einander verschieden, dann stimmt $\Gamma(z, z')$ bis auf eine unwesentliche Constante mit (54) überein.

Die für $\Gamma(z, z')$ aufgestellten Bedingungen führen also darauf, dass diese Function die Gestalt von $G(z, z')$ in (51) besitzt.

§ 650. Nun betrachten wir den grössten gemeinsamen Theiler $K(z, z')$ der beiden ähnlich geformten Ausdrücke

$$\begin{aligned} G(z, z') &= g(z)g_1(z') - g_1(z)g(z'), \\ H(z, z') &= h(z)h_1(z') - h_1(z)h(z'). \end{aligned} \tag{51^a}$$

Es folgt sofort aus dieser Gestalt, dass

$$K(z, z') = \text{const.}\, K(z', z)$$

sein muss. Da ferner

$$G(z, z') = 0, \quad H(z, z') = 0$$

nur verschiedene Wurzeln haben, so hat auch

$$K(z, z') = 0$$

nur unter einander verschiedene Wurzeln $z = z', z_1', \cdots z_{\nu-1}'$. Da endlich

$$K(z, z_\alpha')$$

der grösste gemeinsame Theiler von

$$G(z, z_\alpha'), \quad H(z, z_\alpha')$$

ist, so folgt, dass die Wurzeln von

$$K(z, z_\alpha') = 0$$

sowohl zu denen von

$$G(z, z_\alpha') = 0 \quad \text{als auch von} \quad H(z, z_\alpha') = 0$$

gehören, d. h. dass es wieder $z', z_1', \cdots z_{\nu-1}'$ sind. Es sind also sämmtliche im vorigen Paragraphen für $\Gamma(z, z')$ aufgestellten Bedingungen erfüllt, so dass gesetzt werden kann

$$K(z, z') = k(z)\, k_1(z') - k_1(z)\, k(z'). \tag{55}$$

Da $z', z_1', \cdots z_{\nu-1}'$ zu den Wurzeln jeder der Gleichungen (51ᵃ) gehören, so ist

$$\frac{g(z')}{g_1(z')} = \frac{1}{\nu} \sum_{\alpha=0}^{\nu-1} \frac{g(z_\alpha')}{g_1(z_\alpha')} \quad \text{und} \quad \frac{h(z')}{h_1(z')} = \frac{1}{\nu} \sum_{\alpha=0}^{\nu-1} \frac{h(z_\alpha')}{h_1(z_\alpha')},$$

d. h. beide Brüche auf den linken Seiten der Gleichungen sind rational durch die Coefficienten von (55), d. h. durch $k(z') : k_1(z')$ darstellbar. Es wird demnach, wenn das willkürliche z' durch z ersetzt wird,

$$\frac{g(z)}{g_1(z)} = R_1\left(\frac{k(z)}{k_1(z)}\right); \quad \frac{h(z)}{h_1(z)} = R_2\left(\frac{k(z)}{k_1(z)}\right). \tag{56}$$

Umgekehrt lässt sich auch

$$\frac{k(z)}{k_1(z)} \text{ rational durch } \frac{g(z)}{g_1(z)} \text{ und } \frac{h(z)}{h_1(z)}$$

darstellen. Denn setzt man

$$\frac{g(z')}{g_1(z')} = \lambda, \quad \frac{h(z')}{h_1(z')} = \mu, \tag{57}$$

schreibt die beiden Functionen aus (51ᵃ) in der Form

$$g(z) - g_1(z) \cdot \lambda, \quad h(z) - h_1(z) \cdot \mu \tag{51^b}$$

und sucht dann zu diesen Functionen den grössten gemeinsamen Theiler, indem man λ und μ als willkürliche Parameter betrachtet, so wird der Euklid'sche Algorithmus auf (51^b) eine Reihe von Functionen folgen lassen, die im Allgemeinen mit einer von z unabhängigen Function abschliessen werden. Setzt man in ihnen, von der letzten anfangend und rückwärts gehend, für λ und μ die Werthe (57) ein, so wird die erste dabei nicht verschwindende Function den grössten gemeinsamen Theiler, also (55) geben. Und hierbei erscheint dieser, abgesehen von einem von z unabhängigen Factor, als Function von λ und μ. Damit ist also bewiesen, dass man setzen kann

$$\frac{k(z)}{k_1(z)} = R\left(\frac{g(z)}{g_1(z)}, \frac{h(z)}{h_1(z)}\right).$$

So sind wir auf den Lüroth'schen Satz gekommen: Ist

$$\lambda = \frac{g(z)}{g_1(z)}, \quad \mu = \frac{h(z)}{h_1(z)},$$

dann giebt es eine rationale Function

$$\nu = R(\lambda, \mu)$$

derart, dass man umgekehrt auch

$$\lambda = R_1(\nu), \quad \mu = R_2(\nu)$$

bei rationalen R_1 und R_2 setzen kann.

§ 651. Es seien nun weiter

$$G = \frac{g(z_1, z_2, z_3, \cdots)}{g_1(z_1, z_2, z_3, \cdots)}, \quad H = \frac{h(z_1, z_2, z_3, \cdots)}{h_1(z_1, z_2, z_3, \cdots)}$$

zwei rationale gebrochene Functionen mehrerer Variablen $z_1, z_2, \cdots$ von der Eigenschaft, dass bei der Elimination von z_1 aus

$$g - g_1 \cdot G = 0 \quad \text{und} \quad h - h_1 \cdot H = 0$$

alle z aus g, g_1, h, h_1 verschwinden, so dass die Eliminante

$$\Phi(G, H) = 0$$

von den z frei wird, oder auch, dass zwischen G und H eine von den z unabhängige Gleichung besteht.

Unter $a, b, \cdots$ verstehen wir jetzt willkürliche Constante, unter ζ eine Unbekannte, setzen

$$\mathfrak{g} = \frac{g(\zeta, a, b, \cdots)}{g_1(\zeta, a, b, \cdots)}, \quad \mathfrak{h} = \frac{h(\zeta, a, b, \cdots)}{h_1(\zeta, a, b, \cdots)}$$

und fragen nach den Werthepaaren von $\mathfrak{g}$ und $\mathfrak{h}$, für welche die Gleichungen

$$g(\zeta, a, b, \cdots) - \mathfrak{g} \cdot g_1(\zeta, a, b, \cdots) = 0,$$
$$h(\zeta, a, b, \cdots) - \mathfrak{h} \cdot h_1(\zeta, a, b, \cdots) = 0$$

eine gemeinsame Wurzel ζ haben. Dafür ist es charakteristisch, dass die Resultante der beiden Gleichungen verschwinde. Dies ist nun die oben aufgestellte Function $\Phi(\mathfrak{g}, \mathfrak{h})$, und diese wird für

$$\mathfrak{g} = G, \quad \mathfrak{h} = H$$

wirklich Null. Man kann also einen Werth ζ finden, für den

$$\frac{g(z_1, z_2, \cdots)}{g_1(z_1, z_2, \cdots)} = \frac{g(\zeta, a, \cdots)}{g_1(\zeta, a, \cdots)}; \quad \frac{h(z_1, z_2, \cdots)}{h_1(z_1, z_2, \cdots)} = \frac{h(\zeta, a, \cdots)}{h_1(\zeta, a, \cdots)}$$

wird. Wendet man nun den Lüroth'schen Satz auf die beiden Functionen von ζ an, dann folgt: W e n n d i e F u n c t i o n e n

$$\lambda = \frac{g(z_1, z_2, \cdots)}{g_1(z_1, z_2, \cdots)}, \quad \mu = \frac{h(z_1, z_2, \cdots)}{h_1(z_1, z_2, \cdots)}$$

e i n e r v o n $z_1, z_2, \cdots$ u n a b h ä n g i g e n G l e i c h u n g

$$\Phi(\lambda, \mu) = 0$$

g e n ü g e n, d a n n k a n n m a n e i n e r a t i o n a l e F u n c t i o n f i n d e n

$$\nu = R(\lambda, \mu),$$

d u r c h w e l c h e s i c h r a t i o n a l e r g i e b t

$$\lambda = R_1(\nu), \quad \mu = R_2(\nu).$$

Nun seien drei rationale Functionen G, H, K von $z_1, z_2, z_3, \cdots$ gegeben, zwischen denen zwei von den z unabhängige Relationen

$$\Psi_1(G, H, K) = 0, \quad \Psi_2(G, H, K) = 0$$

bestehen. Eliminirt man G, so gilt der vorige Satz für H und K, d. h. man kann setzen

$$\nu = R(H, K); \quad H = R_2(\nu), \quad K = R_3(\nu)$$

und demnach auch $(\alpha = 1, 2)$

$$\Psi_\alpha(G, R_2(\nu), R_3(\nu)) = 0.$$

Deshalb folgt ebenso

$$\begin{aligned} \pi &= S(G, \nu) = T(G, H, K); \\ \nu &= T_0(\pi), \quad G = T_1(\pi), \\ H &= T_2(\pi), \quad K = T_3(\pi). \end{aligned}$$

Auf diesem Wege kommt man zu dem Gordan'schen Satze*): B e s t e h e n z w i s c h e n m r a t i o n a l e n F u n c t i o n e n v o n n V a r i a b l e n $(m - 1)$ v o n d i e s e n V a r i a b l e n u n a b h ä n g i g e R e l a t i o n e n, s o l ä s s t s i c h e i n e r a t i o n a l e F u n c t i o n j e n e r m F u n c t i o n e n h e r s t e l l e n, d u r c h d i e s i c h u m g e k e h r t e i n e j e d e d e r g e g e b e n e n m F u n c t i o n e n r a t i o n a l d a r s t e l l e n l ä s s t.

*) Math. Ann. 29 (1887), p. 318.

§ 652. Wir gehen nun unserem eigentlichen Ziele entgegen, indem wir die Resolventengleichung für alle conjugen Werthe der Function φ_1

$$F(\varphi) = 0$$

mit den Wurzeln $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ untersuchen, deren Coefficienten nur von einem einzigen Parameter Θ abhängen. Dabei bedeuten also $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ die sämmtlichen conjugen Werthe von φ_1 im Bereiche der symmetrischen Gruppe; sie selbst sowie Θ sind rationale Functionen von n willkürlichen Grössen $z_1, z_2, \cdots z_n$. Ausführlicher können wir also

$$F(\varphi, \Theta) = 0$$

schreiben, wo dann in F ausser φ und Θ nur noch Constante vorkommen. Es ist

$$F(\varphi_\alpha, \Theta) = 0, \quad F(\varphi_\beta, \Theta) = 0$$

für alle $\alpha, \beta = 1, 2, \cdots \varrho$. Eliminirt man aus beiden Gleichungen Θ, so folgt eine Gleichung mit constanten Coefficienten

$$F_1(\varphi_\alpha, \varphi_\beta) = 0,$$

und nun führt uns der obige Gordan'sche Satz sofort zu der Einsicht, dass jedes der φ_α sich rational durch eine Grösse ψ ausdrücken lässt, welche umgekehrt aus ihnen rational gebildet werden kann. Wir schreiben dies

$$\psi = T(\varphi_1, \varphi_2, \cdots \varphi_\varrho);$$
$$\varphi_1 = T_1(\psi), \quad \varphi_2 = T_2(\psi), \quad \cdots \quad \varphi_\varrho = T_\varrho(\psi).$$

Ist $n > 4$, dann muss ψ zur Gruppe 1 gehören, da sonst gegen § 543 die Gruppen der Functionen $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ sämmtlich eine Substitution gemeinsam hätten, die von der Einheit verschieden ist. ψ wird also eine Galois'sche Function von $n!$ Werthen, und alle

$$\psi_i = T\left(\varphi_{i_1}, \varphi_{i_2}, \cdots \varphi_{i_\varrho}\right),$$

welche durch Einwirkung irgend einer Substitution s_i der z aus ψ hervorgehen, sind unter einander verschieden.

Nun stimmt die Reihe der Argumente $\varphi_{i_1}, \varphi_{i_2}, \cdots \varphi_{i_\varrho}$ mit der Reihe $\varphi_1, \varphi_2, \cdots \varphi_\varrho$ bis auf die Folge überein, und die $\varphi_1, \varphi_2, \cdots$ sind Functionen von ψ. Folglich muss sein

$$\psi_i = Q_i(\psi).$$

Da auch die umgekehrten Schlüsse gelten, wie die Betrachtung von

$$\varphi_{i_1} = T_1(\psi_i), \quad \varphi_{i_2} = T_2(\psi_i), \quad \cdots \quad \varphi_{i_\varrho} = T_\varrho(\psi_i)$$

zeigt, so ergiebt sich: Jeder der conjugen Werthe $\psi_1, \psi_2, \cdots \psi_{n!}$ ist eine rationale Function jedes anderen.

Daraus folgt, dass ein jeder eine lineare gebrochene Function jedes anderen ist. Denn setzen wir

$$\psi_\alpha = \frac{M(\psi_\beta)}{N(\psi_\beta)}, \quad \psi_\beta = \frac{M_1(\psi_\alpha)}{N_1(\psi_\alpha)},$$

so folgt bei Substitution des zweiten Werthes von ψ_β in die erste Gleichung, weil dadurch eine Identität entstehen müsste, und also rechts gekürzt werden könnte, der ausgesprochene Satz nach § 273, Bd. I. Folglich ist, immer mit constanten Coefficienten,

$$\psi_\alpha = \frac{a\psi_\beta + b}{c\psi_\beta + d}, \quad \psi_\beta = \frac{d\psi_\alpha - b}{-c\psi_\alpha + a}.$$

§ 653. Wir wählen nun einen beliebigen Werth ψ aus und setzen

$$\psi = \frac{h(z_1, z_2, \cdots z_n)}{k(z_1, z_2, \cdots z_n)},$$

wobei h und k ganze Functionen der Argumente z ohne gemeinsamen Theiler sein sollen. Ebenso schreiben wir

$$\psi_i = \frac{h(z_{i_1}, z_{i_2}, \cdots)}{k(z_{i_1}, z_{i_2}, \cdots)} = \frac{h_i(z_1, z_2, \cdots)}{k_i(z_1, z_2, \cdots)}.$$

Es ist nun nach der letzten Gleichung des vorigen Paragraphen

$$\frac{h_i}{k_i} = \frac{a_i h + b_i k}{c_i h + d_i k},$$

und da h mit k keinen gemeinsamen Theiler hat, so hat einen solchen auch h_i nicht mit k_i und ebenso wenig $(a_i h + b_i k)$ mit $(c_i h + d_i k)$. Folglich sind bis auf constante Factoren die beiden Zähler der letzten Gleichung einander gleich und auch die beiden Nenner. Diese constanten Factoren können wir mit a_i, b_i bezw. c_i, d_i vereint denken und dürfen

$$h_i = a_i h + b_i k, \quad k_i = c_i h + d_i k$$

schreiben. Dies gilt für beliebige Indices i, so dass wir

$$h_i = a_i h + b_i k,$$
$$h_j = a_j h + b_j k$$

setzen können. Ist $a_i b_j - a_j b_i$ von Null verschieden, so liefert die Elimination von k eine lineare Beziehung zwischen h, h_i und h_j. Ist dagegen $a_i b_j = b_i a_j$, so gilt schon eine lineare Beziehung zwischen

h_i und h_j. In beiden Fällen also giebt es zwischen drei willkürlichen conjugen Functionen h, h_i, h_j eine Relation

$$\alpha \cdot h + \beta \cdot h_i + \gamma \cdot h_j = 0,$$

in welcher mindestens zwei der Coefficienten von 0 verschieden sind. Man kann daher jede der conjugen Functionen $h_1, h_2, h_3, \cdots$ durch zwei willkürlich gewählte h_i, h_k in der Form

$$h_\alpha = a_\alpha h_i + b_\alpha h_k \qquad (\alpha = 1, 2, 3, \cdots) \tag{64}$$

darstellen.

§ 654. Um hieraus weitere Schlüsse ziehen zu können, wollen wir ein allgemeines Theorem über die conjugen Gruppen (§ 541) einer Gruppe G_1

$$G_1, \; G_2, \; G_3, \; \cdots \; G_\varrho$$

ableiten. Der Satz gehört zu dem in § 543 behandelten und lautet: Jede Gruppe G_1 von Substitutionen aus n Elementen hat mit einer ihrer conjugen Gruppen noch von der Einheit verschiedene Substitutionen gemeinsam, wenn $n > 4$ ist.

Gesetzt G_1 besässe mit jeder der Gruppen $G_2, G_3, \cdots G_\varrho$ der n Elemente $z_1, z_2, \cdots z_n$ immer nur die Einheitssubstitution gemeinsam, dann sei s eine Substitution aus G_1, welche möglichst wenige, nämlich nur $(n - \nu)$ Elemente umsetzt, wobei $\nu < n$ sei.

Wir betrachten zuerst den Fall $\nu \geqq 2$. Dann giebt es eine Transposition $t = (z_\alpha z_\beta)$ aus zwei in s nicht vorkommenden Elementen. Nun wird wegen der Form von s die Transformirte

$$t^{-1} s t = (z_\alpha z_\beta)^{-1} \cdot s \cdot (z_\alpha z_\beta) = s;$$

und wenn t nicht zu G_1 gehörte, dann hätte G_1 mit $G_t = t^{-1} G_1 t$ die Substitution s gegen die Voraussetzung gemeinsam. Folglich muss $t = (z_\alpha z_\beta)$ in G_1 vorkommen. Ist jetzt $n > 4$, nimmt man für die eben betrachtete Substitution s das t, dessen Vorkommen in G_1 soeben nachgewiesen worden ist, dann zeigen dieselben Schlüsse, dass G_1 alle Transpositionen und also die symmetrische Gruppe umfasst. Hierfür wird das Theorem gegenstandslos.

Ist dagegen $n \leqq 4$, dann zeigt sich leicht, dass der Satz nicht mehr gültig bleibt.

Wir betrachten nun den Fall $\nu \leqq 1$. Die Gruppe G_1 enthält dabei nur reguläre Substitutionen, d. h. solche, die aus Cyklen von derselben Ordnung bestehen. Ist zuerst $\nu = 1$, dann ist entweder n oder $n - 1$ keine Primzahl; daher giebt es eine reguläre Substitution

in G, die nicht von Primzahlordnung ist, und sie oder eine ihrer Potenzen enthält mehrere Cyklen, z. B.

$$(z_1 z_2 z_3)(z_4 z_5 z_6)\cdots.$$

Transformirt man nun in diesem Falle durch einen der Cyklen, z. B. hier durch $(z_1 z_2 z_3)$, so reproducirt sich die Substitution. Also müsste nach den obigen Schlüssen gegen die Voraussetzung der Cyklus selbst als Substitution zur Gruppe G_1 gehören. Es kann demnach nicht $\nu = 1$ sein.

Ist endlich $\nu = 0$, so besteht G_1 aus Substitutionen, die alle oder kein Element umstellen; hier reichen dieselben Ueberlegungen aus, auch wenn die Substitutionen nur aus einem Cyklus bestehen, indem man z. B., wenn n eine Primzahl ist,

$$s = (z_1 z_2 z_3 \cdots z_n)$$

durch

$$t = (z_1)(z_2 z_n)(z_3 z_{n-1})\cdots$$

transformirt. Unser Satz ist also in allen Fällen bewiesen.

§ 655. Wählen wir nun in den Betrachtungen des § 653 über die Resolventen mit einem Parameter für die Formel (64) h_i und h_k so, dass ihre Gruppen ausser der Einheit noch andere Substitutionen gemeinsam haben, dann würden gemäss dieser Formel alle Gruppen der $h_1, h_2, h_3, \cdots$ dieselben Substitutionen gemein haben. Das widerspricht dem Satze § 543. Folglich giebt es, wenn $n > 4$ ist, keine Gleichungen für Resolventen, die nur von einem einzigen Parameter abhängen.

Bei $n = 4$ treten Functionen auf, deren Gleichung nur einen Parameter aufweist. Nehmen wir die Functionen

$$\varphi_1 = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_2 - z_3)(z_1 - z_4)},$$

so werden ihre conjugen Werthe die folgenden

$$\varphi_2 = \frac{(z_2 - z_3)(z_1 - z_4)}{(z_1 - z_3)(z_2 - z_4)} = \frac{1}{\varphi_1};$$

$$\varphi_3 = \frac{(z_1 - z_2)(z_3 - z_4)}{(z_3 - z_2)(z_1 - z_4)} = 1 - \varphi_1;$$

$$\varphi_4 = \frac{(z_3 - z_2)(z_1 - z_4)}{(z_1 - z_2)(z_3 - z_4)} = \frac{1}{1 - \varphi_1};$$

$$\varphi_5 = \frac{(z_1 - z_3)(z_4 - z_2)}{(z_4 - z_3)(z_1 - z_2)} = \frac{\varphi_1}{1 - \varphi_1},$$

$$\varphi_6 = \frac{(z_4 - z_3)(z_1 - z_2)}{(z_1 - z_3)(z_4 - z_2)} = \frac{1 - \varphi_1}{\varphi_1}.$$

Diese sechs Grössen $\varphi_1, \varphi_2, \cdots \varphi_6$ sind die Wurzeln der Gleichung

$$\varphi^6 - 3\varphi^5 + A \cdot \varphi^4 - (2A - 5)\varphi^3 + A\varphi^2 - 3\varphi + 1 = 0,$$

in welcher A eine symmetrische Grösse in z_1, z_2, z_3, z_4 bedeutet, die durch

$$2A = \left(\sum \varphi_\alpha\right)^2 - \sum \varphi_\alpha^2$$
$$= 9 - \sum \varphi_\alpha^2$$

berechnet werden kann. Die obige Gleichung zeigt auch, dass

$$A = -\frac{\varphi_\alpha^6 - 3\varphi_\alpha^5 + 5\varphi_\alpha^3 - 3\varphi_\alpha + 1}{\varphi_\alpha^4 - 2\varphi_\alpha^3 + \varphi_\alpha^2} \qquad (\alpha = 1, 2, \cdots 6)$$

eine symmetrische Function der φ_α oder auch der z_α ist.

Namen- und Sachregister.

(Die lateinischen Zahlen beziehen sich auf den Band, die deutschen auf die Seite.)

VORLESUNGEN

ÜBER

ALGEBRA

VON

DR. EUGEN NETTO,
O. Ö. PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT ZU GIESSEN.

IN ZWEI BÄNDEN.

ERSTE LIEFERUNG DES ZWEITEN BANDES.

MIT EINGEDRUCKTEN HOLZSCHNITTEN.

LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1898.

Die II. (Schluss-) Lieferung erscheint im Februar 1899.

Vorbemerkung.

Die zunächst erscheinende erste Abtheilung des zweiten Bandes der Vorlesungen über Algebra ist der Theorie der Functionen und der Gleichungen mehrerer Variablen und Unbekannten gewidmet. Auf die Definition der Function folgen zunächst Erörterungen über die Gliederzahl und daran sich anknüpfende Probleme, dann die Fragen nach der Interpolation, nach der Reductibilität, nach gemeinsamen Theilern. Beim Begriffe von Wurzeln muss der neue Umstand der unendlich grossen Wurzeln in Erwägung gezogen werden. Daran schliesst sich durch Uebergang zu mehreren Gleichungen naturgemäss die Behandlung der Elimination. Hier hat der Verfasser es für nützlich gehalten, die bisher unterschiedlos benutzten Ausdrücke „Eliminante“ und „Resultante“ begrifflich zu trennen. Die drei Hauptmethoden der Elimination werden eingehend besprochen: die Bézout'sche, die Cramer-Poisson'sche, die Kronecker'sche; einer kritischen Besprechung wird auch die Cayley'sche unterzogen. Zur Darstellung der Poisson'schen Methode war eine Besprechung der symmetrischen Functionen mehrerer Grössenreihen nothwendig. Auch bei Gleichungssystemen muss der Begriff der vielfachen und der unendlichen Wurzeln erläutert werden; dies geschieht im Anschluss an die Resultante und die Eliminante, welche in das Centrum der Untersuchung gerückt werden. Der Versuch einer Erweiterung des Discrimantenbegriffes führt zu zwei Ergebnissen, einmal hinsichtlich vielfacher Wurzeln eines Systems, dann hinsichtlich singulärer Punkte eines einzelnen Gebildes. Die Irreductibilität und Reductibilität, die Stufenzahl, die Abhängigkeit und Unabhängigkeit von Gleichungssystemen wird besprochen und das Jacobi'sche Theorem, welches als Erweiterung Euler'scher Formeln auftritt, auf verschiedene Weise abgeleitet. Den Schluss bildet eine Darstellung der Kronecker'schen Charakteristiken-Theorie sowie der Hermite'schen Untersuchungen über die quadratischen Formen.

So bald als möglich soll die zweite Abtheilung, welche die allgemeine Theorie der algebraischen Gleichungen einer Unbekannten bringt, dieser ersten Abtheilung folgen.

Giessen.

E. Netto.

Inhalt der ersten Lieferung des zweiten Bandes.

Inhalt der ersten Lieferung des zweiten Bandes.

VORLESUNGEN

ÜBER

ALGEBRA

VON

DR. EUGEN NETTO,
O. Ö. PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT ZU GIESSEN.

IN ZWEI BÄNDEN.

ZWEITE (SCHLUSS-)LIEFERUNG DES ZWEITEN BANDES.

LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1900.

Festschrift zu Moritz Cantors 70. Geburtstage. Zugleich 9. Heft d. Abhandl. z. Gesch. d. Mathem. u. Supplement z. 44. Jahrg. d. Zeitschr. f. Mathem. u. Physik. [VIII u. 657 S.] gr. 8. 1899. geh. n. ℳ 20.—

——— zur Feier der Enthüllung des Gauss-Weber-Denkmals in Göttingen. Herausg. vom Fest-Comitee. Lex.-8. 1899. geh. n. ℳ 6.—. Enthaltend: **Hilbert**, D., Grundlagen der Geometrie [92 S.]; **Wiechert**, E., Grundlagen d. Elektrodynamik [112 S.].

Föppl, Dr. **A.**, Professor an der Technischen Hochschule zu München, Vorlesungen über technische Mechanik. 4 Bde. gr. 8. In Leinwand geb.

I. Band: Einführung in d. Mechanik. M. 78 Fig. i. T. [XV u. 412 S.] 1898. n. ℳ 10.—
II. Band: Graphische Statik. [In Vorbereitung.]
III. Band: Festigkeitslehre. Mit 70 Figuren im Text. [XVI u. 472 S.] 1897. n. ℳ 12.—
IV. Band: Dynamik. Mit 69 Figuren im Text. [XIV u. 456 S.] 1899. n. ℳ 12.—

Genocchi, Angelo, Differentialrechnung und Grundzüge der Integralrechnung, herausgegeben von Giuseppe Peano. Autorisierte deutsche Uebersetzung von G. Bohlmann und A. Schepp. Mit einem Vorwort von A. Mayer. [VIII u. 399 S.] gr. 8. 1899. In Leinw. geb. n. ℳ 12.—

Holzmüller, Prof. Dr. **Gustav**, Direktor der Kgl. Maschinenbauschule zu Hagen, Mitglied der Leopoldinisch-Karolinischen Akademie, die Ingenieur-Mathematik in elementarer Behandlung. 2 Teile. II. Teil, enthaltend das Potential und seine Anwendung auf die Theorien der Gravitation, des Magnetismus, der Elektricität, der Wärme und der Hydrodynamik. Mit 237 Figuren, zahlreichen Übungsbeispielen und einem Anhange über die Maſseinheiten. [XVII u. 440 S.] gr. 8. 1898. In Lnw. geb. n. ℳ 6.—

Kohlrausch, Professor Dr. **F.**, Präsident der physikalisch-technischen Reichsanstalt in Charlottenburg, kleiner Leitfaden der praktischen Physik. Für den Unterricht in den physikalischen Übungen. Mit in den Text gedruckten Figuren. [XIX u. 260 S.] gr. 8. 1899. In Leinw. geb. n. ℳ 4.—

Krause, Dr. **Martin**, Professor an der Königl. Sächs. Technischen Hochschule zu Dresden, Theorie der doppeltperiodischen Functionen einer veränderlichen Grösse. (In 2 Bänden.) Zweiter Band. [XII u. 306 S.] gr. 8. 1897. geh. n. ℳ 12.—

Kronecker's, Leopold, Werke. Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von K. Hensel. (In 4 Bänden.) Dritter Band. I. Halbband. [VIII u. 474 S.] gr. 4. 1899. geh. n. ℳ 36.— [Der zweite Halbband befindet sich u. d. Pr.]

Mansion, Prof. Dr. **P.**, Gent, Einleitung in die Theorie der Determinanten. Für Gymnasien und Realschulen. Aus der 3. franz. Aufl. übersetzt. [40 S.] gr. 8. 1899. geh. n. ℳ 1.—

Muth, Dr. **P.**, Osthofen, Theorie und Anwendung der Elementarteiler. [XVI u. 236 S.] gr. 8. 1899. geh. n. ℳ 8.—

Netto, Dr. **Eugen**, o. ö. Professor der Mathematik an der Universität zu Gieſsen, Vorlesungen über Algebra. In zwei Bänden. II. Band. 2. (Schluſs-)Lieferung. [XI u. S. 193—327.] gr. 8. 1900. geh. n. ℳ 10.—.

Neumann, Dr. **C.**, Professor der Mathematik an der Universität zu Leipzig, die elektrischen Kräfte. Darlegung und genauere Betrachtung der von hervorragenden Physikern entwickelten mathematischen Theorieen. Zweiter Theil: Ueber die von Hermann von Helmholtz in seinen älteren und in seinen neueren Arbeiten angestellten Untersuchungen. [XXXVIII u. 462 S.] gr. 8. 1898. geh. n. ℳ 14.—

Pascal, Ernst, o. Prof. a. d. Univ. zu Pavia, die Variationsrechnung. Autorisierte deutsche Ausgabe von Adolf Schepp, Ingenieur und Oberleutnant a. D. zu Wiesbaden. [VI u. 146 S.] gr. 8. 1899. In Leinwand geb. n. ℳ 3.60.

Riemann, B., elliptische Funktionen. Vorlesungen herausg. von Prof. Dr. H. Stahl, Tübingen. Mit Figuren im Text. [VIII u. 144 S.] gr. 8. 1899. geh. n. ℳ 5.60.

Routh, John Edward, Sc. D., Ll. D., F. R. S., etc.; Ehrenmitglied von Peterhouse, Cambridge; Mitglied des Senats der Universität London, die Dynamik der Systeme starrer Körper. In zwei Bänden mit zahlreichen Beispielen. Autorisierte deutsche Ausgabe von Adolf Schepp. Mit einem Vorwort von Felix Klein. 2 Bände. gr. 8. In Leinwand geb. n. M. 24.—

I. Band: Die Elemente. Mit 57 Fig. im Text. [XII u. 472 S.] 1897. n. M. 10.—
II. Band: Die höhere Dynamik. Mit 38 Fig. im Text. [X u. 544 S.] 1898. n. M. 14.—

Rudio, Dr. Ferd., Prof. am Polytechnikum in Zürich, die Elemente der analytischen Geometrie. Zum Gebrauche an höheren Lehranstalten sowie zum Selbststudium. Mit zahlreichen Uebungsbeispielen. Zweiter Teil: Die analytische Geometrie des Raumes. Mit 12 Fig. im Text. Zweite verbesserte Auflage. [X u. 184 S.] gr. 8. 1899. geh. n. M. 2.40; in Leinwand geb. n. M. 3.—

Salmon, George, analytische Geometrie des Raumes. Deutsch bearbeitet von Dr. Wilhelm Fiedler, Professor am Eidgenössischen Polytechnikum zu Zürich. Zwei Teile. I. Teil: Die Elemente und die Theorie der Flächen zweiten Grades. Vierte verbesserte Auflage. [XXIV u. 448 S.] gr. 8. 1898. geh. n. M. 8.—

——— analytische Geometrie der Kegelschnitte mit besonderer Berücksichtigung der neueren Methoden. Nach George Salmon frei bearbeitet von Dr. Wilhelm Fiedler, Professor am Eidgenössischen Polytechnikum zu Zürich. In 2 Teilen. I. Teil. Sechste verbess. Aufl. [XXV u. 442 S.] gr. 8. 1898. geh. n. M. 9.—

Scheibner, W., über die Differentialgleichungen der Mondbewegung. (Abhandl. d. math.-phys. Classe d. Kgl. Sächs. Ges. d. Wissensch., XXV. Bd. Nr. II.) [II u. 26 S.] Lex.-8. 1899. geh. n. M. 1.50.

Schell, W., allgemeine Theorie der Curven doppelter Krümmung in rein geometrischer Darstellung. Zur Einführung in das Studium der Curventheorie. 2. erweiterte Auflage. [VIII u. 163 S.] gr. 8. 1898. geh. n. M. 5.—

Serret, J.-A., † Membre de l'Institut et du Bureau des Longitudes à Paris, Lehrbuch der Differential- u. Integral-Rechnung. Mit Genehmigung des Verfassers deutsch bearbeitet von Dr. Axel Harnack, † Prof. an der Technischen Hochschule zu Dresden. Zweite, durchgesehene Auflage mit Unterstützung der Herren H. Liebmann u. E. Zermelo herausgegeben von Dr. G. Bohlmann, Privatdocent an der Universität zu Göttingen. In drei Bänden. gr. 8. geh.

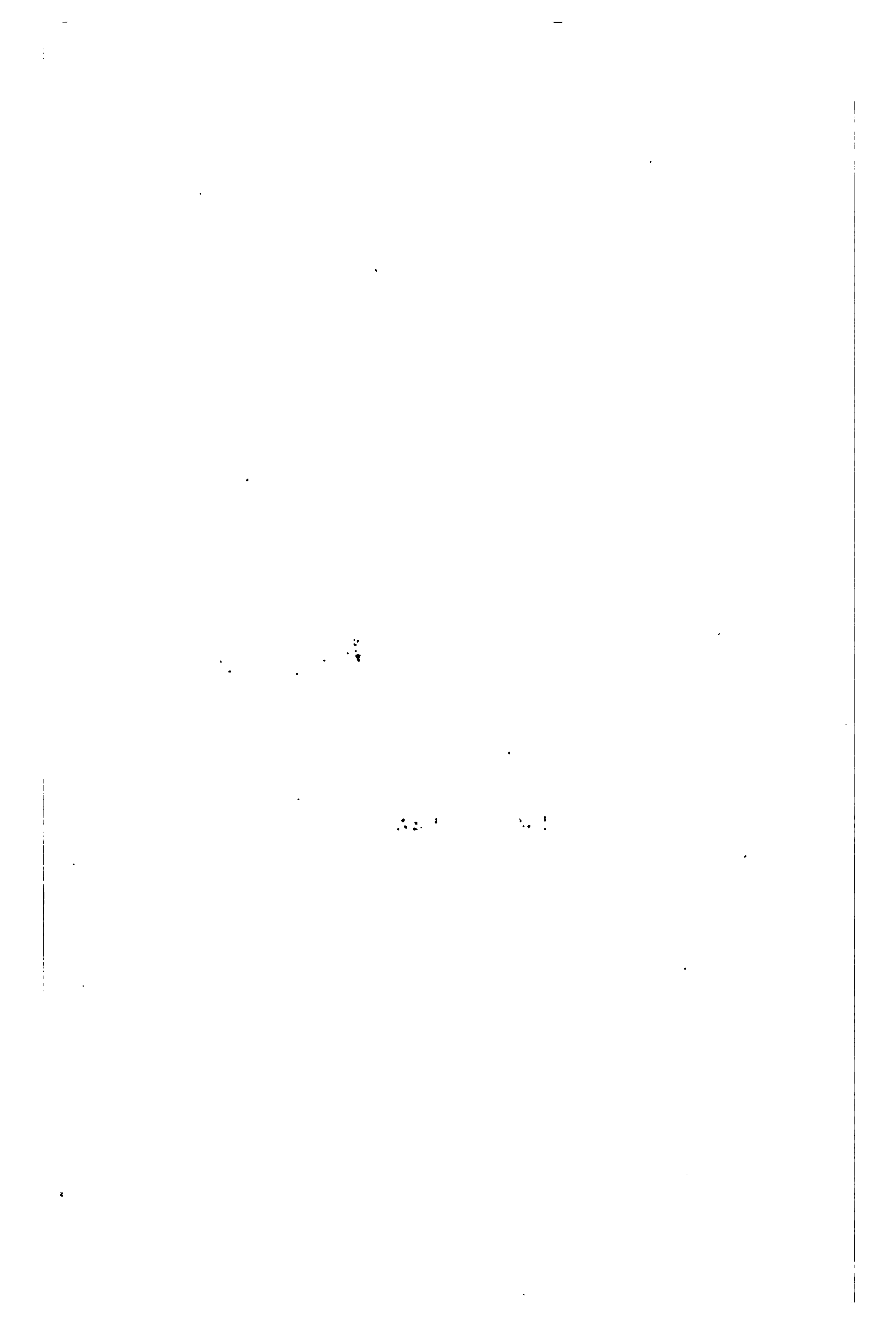
I. Band: Differentialrechnung. Mit 85 Fig. im Text. [X u. 570 S.] 1897. n. M. 10.—
II. Band: Integralrechnung. Mit 55 Fig. im Text. [XII u. 428 S.] 1899. n. M. 8.—
III. Band: Differentialgleichungen und Variationsrechnung. [In Vorbereitung.]

Steiner's, Jacob, Vorlesungen über synthetische Geometrie. 2 Teile. II. Teil: Die Theorie der Kegelschnitte, gestützt auf projektive Eigenschaften. Auf Grund von Universitätsvorträgen und mit Benutzung hinterlassener Manuscripte Jacob Steiner's bearb. von Heinrich Schröter. 3. Aufl. von Rudolf Sturm. Mit 103 Figuren im Text. [XVII u. 538 S.] gr. 8. 1898. geh. n. M. 14.—

Stolz, Dr. Otto, ord. Professor an der Universität zu Innsbruck, Grundzüge der Differential- und Integralrechnung. In 3 Teilen. III. Teil: Die Lehre von den Doppelintegralen. Eine Ergänzung zum I. Teile des Werkes. Mit 41 Figuren im Text. [VIII u. 296 S.] gr. 8. 1899. geh. n. M. 8.—

Volkmann, Dr. P., o. ö. Professor der theoretischen Physik an der Universität Königsberg i. Pr., Einführung in das Studium der theoretischen Physik, insbesondere in das der analytischen Mechanik. Mit einer Einleitung in die Theorie der physikalischen Erkenntnis. Vorlesungen. [XVI u. 370 S.] gr. 8. 1900. geh. n. M. 14.—

von Weber, Dr. E., Privatdocent an der Universität München, Vorlesungen über das Pfaff'sche Problem und die Theorie der partiellen Differentialgleichungen erster Ordnung. gr. 8. geh. [Erscheint im März 1900.]




NOV 30 1909
DEC 3 - 1901
JAN 24 1922
JUL 16 1912
DUE MAY 17 1920
FOR USE IN
BUILDING

